universität
wien

DIPLOMARBEIT

Titel der Diplomarbeit

Hilbert's tenth problem over subrings of $\mathbb{Q}$

angestrebter akademischer Grad

Magister der Naturwissenschaften (Mag. rer. nat.)

Verfasser:	Stefan Perlega
Matrikel-Nummer:	0402537
Studienkennzahl (lt. Studienblatt):	A 405
Studienrichtung (lt. Studienblatt):	Mathematik
Betreuer:	Ao. Univ.-Prof. Dr. Christoph Baxa

Wien, am 26. 01. 2011

Contents

The following notational conventions will be used:

- $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- $\mathcal{P}$ will denote the set of prime numbers.
- For $n \in \mathbb{N}$ let $\pi_{\mathbb{Q}}(n) := \#\{p \in \mathcal{P} | p \leq n\}$.
- For any field K let $\overline{K}$ denote its algebraic closure.
- For integers $x_1, \ldots, x_n \neq 0$ let $(x_1, \ldots, x_n)$ denote their greatest common divisor.
- Every ring R is assumed to be commutative with unity $1 \neq 0$ and an integral domain. If we want to emphasize that we speak of elements of R (and not of $\mathbb{N}$), we will sometimes write 0_R for the zero-element and 1_R for the unity of R.
- For a tuple $(x_1, \ldots, x_n) \in X^n$ we will often just write x.
- For a map $f : X \to Y$ we define the map $\bar{f} : X^n \to Y^n$ as $\bar{f}(x_1, \ldots, x_n) := (f(x_1), \ldots, f(x_n))$. (the n will be suppressed in this notation.)
- For a subset $A \subseteq X$ its characteristic function $\chi_A : X \to \{0, 1\}$ is defined as

$$\chi_A(x) := \begin{cases} 1 & x \in A \\ 0 & x \notin A. \end{cases}$$

  (the superset X will be suppressed in this notation.)
- For a subset $A \subseteq R^n$ (with R a ring) we define a special characteristic function χ_A^R where $\chi_A^R : R^n \to \{0_R, 1_R\}$ in the same way.
- If $p \in \mathcal{P}$, then $|.|_p$ will denote the p-adic valuation on $\mathbb{Q}$, $|x|_p := p^{-\operatorname{ord}_p(x)}$. Further, $|x|_\infty = |x|$ will denote the absolut value of $x \in \mathbb{Q}$.
- $\mathbb{Q}_p$ will denote the field of p-adic numbers with the subsets: $\mathbb{Z}_p := \{x \in \mathbb{Q}_p | \operatorname{ord}_p(x) \geq 0\}$, $\mathcal{M}_p := \{x \in \mathbb{Q}_p | \operatorname{ord}_p(x) > 0\}$, $\mathcal{M}_p^n := \{x \in \mathbb{Q}_p | \operatorname{ord}_p(x) \geq n\}$ for $n \geq 1$.
- More generally, if K is a finite extension of $\mathbb{Q}$ and $\mathfrak{p}$ a prime of K, then let $K_\mathfrak{p}$ denote the completion of K under the corresponding $\mathfrak{p}$-adic value. Further, $\mathcal{O}_K$ will denote the ring of algebraic integers in K and $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$.
- If K, L are two fields with $K \subseteq L$, then $\operatorname{Gal}(L/K)$ will denote the Galois group of L over K.
- For any field K let $\mathbb{P}^n(K)$ denote the n-dimensional projective space over K. Let the elements of $\mathbb{P}^n(K)$ be denoted as $(x_0 : \ldots : x_n)$.

1 Hilbert's tenth problem and its solution

1.1 Introduction and formulation of the problem

In 1900 David Hilbert presented a list of 23 unsolved problems at the International Congress of Mathematicians. His aim was to call the attention of his audience to a number of topics of which he thought would play an important role in the progress of mathematics in the following century. The tenth problem on his list was formulated in the following way:
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.
In modern terminology, Hilbert asked for an algorithm which decides if a given diophantine equation is solvable. Thus, we can formulate the problem in the following way:

Problem 1.1.1 (H10)**.** Is there an *algorithm* which takes the coefficients of a polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ (with $n \geq 1$ arbitrary) as input and decides whether there is an $x \in \mathbb{Z}^n$ such that $f(x) = 0$?

If we want to feed our algorithm with polynomials $f \in \mathbb{Z}[x_1, \ldots, x_n]$, with n an arbitrary positive integer, we need to fix a unique way of encoding polynomials with integer coefficients in arbitrarily many variables as tuples of integers. A convenient way to do this is to use the first entry of the tuple to denote the degree of the polynomial, the second entry to denote the number of variables and to use the remaining entries for the coefficients of the polynomial in lexicographic order. This means that the polynomial

$$f(x) = \sum_{0 \leq i_1, \ldots, i_n \leq d} a_{i_1, \ldots, i_n} x_1^{i_1} \cdots x_n^{i_n}$$

would be encoded as

$$(d, n, a_{0,\ldots,0}, a_{0,\ldots,0,1}, \ldots, a_{0,\ldots,0,d}, a_{0,\ldots,0,1,0}, \ldots, a_{0,\ldots,0,1,d}, a_{0,\ldots,0,2,0}, \ldots, a_{d,\ldots,d}).$$

For example, we would encode

$$(x^3 - 3x^2 + 3x - 1) \longmapsto (3, 1, -1, 3, -3, 1),$$

$$(x^2 + y^2 - 1) \longmapsto (2, 2, -1, 0, 1, 0, 0, 0, 1, 0, 0).$$

This gives us a mapping $C_{\mathbb{Z}} : \bigcup_{n \geq 1} \mathbb{Z}[x_1, \ldots, x_n] \to \bigcup_{n \geq 1} \mathbb{Z}^n$.

Using the notion of computable functions, we can rephrase the original problem in the following way:

Problem 1.1.2 (H10)**.** Is there a *computable* function $T : \bigcup_{n\geq 1} \mathbb{Z}^n \to \{0,1\}$ such that $T(t) = 1$ if and only if the following conditions are fulfilled:

- There is a $m \geq 1$ and a $f \in \mathbb{Z}[x_1, \ldots, x_m]$ such that $C_{\mathbb{Z}}(f) = t$.
- There is a $x \in \mathbb{Z}^m$ with $f(x) = 0$.

In 1970 Yuri Matiyasevich proved that there is no such function. Therefore, he gave a negative answer to Hilbert's tenth problem. We also say that Hilbert's tenth problem is *undecidable*.
The question posed in Hilbert's tenth problem has been generalized by asking for algorithms which determine if a polynomial equation over a ring R other than $\mathbb{Z}$ has solutions over R. We call this related problem Hilbert's tenth problem (or H10) over R. The answer to this problem seems to be heavily dependent on the diophantine structure of R. While H10 has been solved over numerous rings, it still remains unsolved over others (most importantly, over $\mathbb{Q}$).
The second chapter of this thesis will be dedicated to the general problem of H10 over rings R other than $\mathbb{Z}$. We will introduce methods which will allow us to solve this problem in certain cases. The remaining two chapters of the thesis will deal with H10 over subrings of $\mathbb{Q}$. In chapter 3 we will discuss a recent result by Bjorn Poonen which proves H10 to be undecidable over certain large subrings of $\mathbb{Q}$. The proof heavily makes make use of the theory of elliptic curves. In chapter 4 we will discuss another recent result by Kirsten Eisenträger and Graham Everest which shows that one can construct two subrings R_1, R_2 of $\mathbb{Q}$ such that $R_1 \cdot R_2 = \mathbb{Q}$ and that H10 is undecidable over R_1 and R_2. Further, these rings are complementary in a strong sense. Again, the proof will involve elliptic curves.
In the remainder of the first chapter we will introduce several elementary notions of computability theory which will be needed in our discussion of Hilbert's tenth problem. To conclude this chapter, we will also shortly discuss the proof of the fact that H10 is undecidable (over $\mathbb{Z}$) and introduce the fundamental notion of diophantine sets.

1.2 Computable functions, computable sets and listable sets

Our main references for questions of computability will be chapter 1 and chapter 5 of [11], chapter 7 of [4] and the appendix A of [15].
In order to fully understand Problem 1.1.2 we need to understand what it means for a function to be computable. We start by defining the μ-Operator.

Definition 1.2.1. Let $R(x_1, \ldots, x_n, y)$ be a relation on $\mathbb{N}$ (thus, a map $R : \mathbb{N}^{n+1} \to \{0,1\}$) for some $n \geq 1$ with the property

$$\forall x \in \mathbb{N}^n \exists y \in \mathbb{N} : R(x,y) = 1. \tag{1.2.1}$$

Then we define for $x \in \mathbb{N}^n$ the mapping

$$\mu_y(R(x,y)) := \min\{y \in \mathbb{N} | R(x,y) = 1\}.$$

Definition 1.2.2 (Computable functions)**.** Let $\mathcal{F}_n := \{f | f \text{ is a map } \mathbb{N}^n \to \mathbb{N}\}$ and $\mathcal{F} := \bigcup_{n\geq 0} \mathcal{F}_n$ (with $\mathcal{F}_0 \cong \mathbb{N}$ the constant functions). Then we define the set of computable functions (also called recursive functions) as the smallest subset of $\mathcal{F}$ which contains the following functions:

(1) every constant function $f \in \mathcal{F}_0$, $f = a$ with $a \in \mathbb{N}$,

(2) the successor function $f \in \mathcal{F}_1$, $f(x) := x + 1$,

(3) the projections $\pi_i \in \mathcal{F}_n$, $\pi_i(x_1, \ldots, x_n) := x_i$ for all $n \geq 1$ and $i \in \{1, \ldots, n\}$,

and is closed under the following operations:

(1) Composition: For computable functions $g \in \mathcal{F}_m$ and $f_1, \ldots, f_m \in \mathcal{F}_n$ the function $h \in \mathcal{F}_n$,

$$h(x) := g(f_1(x), \ldots, f_m(x))$$

is also computable.

(2) Inductive definition: For computable functions $f_0 \in \mathcal{F}_n$ and $g \in \mathcal{F}_{n+2}$ the function $f \in \mathcal{F}_{n+1}$ defined by

$$f(x_1, \ldots, x_n, y) := \begin{cases} f_0(x_1, \ldots, x_n) & y = 0 \\ g(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y-1)) & y \geq 1 \end{cases} \tag{1.2.2}$$

is also computable.

(3) Minimization: Let $R(x_1, \ldots, x_n, y)$ be a computable relation on $\mathbb{N}$ satisfying (1.2.1). Then $\mu_y(R(x, y))$ is also computable.

Further, we will call a function $f : \mathbb{N}^n \to \mathbb{N}^m$, $f(x) = (f_1(x), \ldots, f_m(x))$ computable if the functions $f_1, \ldots, f_m$ are computable.
Also, a function $f : \mathbb{N}^n \to \bigcup_{m\geq 1} \mathbb{N}^m$ will be called computable if there is a computable function $h : \mathbb{N}^n \to \mathbb{N}$ such that $h(x) = k$ if and only if $f(x) \in \mathbb{N}^k$ and the function $g : \mathbb{N}^{n+1} \to \mathbb{N}$ is computable, where g is defined by $g(x, i) := \pi_{i_0}(f(x))$ with $1 \leq i_0 \leq h(x)$ and $i \equiv i_0 \pmod{h(x)}$.
Finally, a function f with domain $\bigcup_{n\geq 1} \mathbb{N}^n$ is called computable if the restriction of f to $\mathbb{N}^n$ is a computable function for all $n \geq 1$.

We now want to show that some basic functions, which will be used later on, are computable.

Lemma 1.2.3. *Let $f(x_1, \ldots, x_n) : \mathbb{N}^n \to \mathbb{N}$ be a computable function. Then for any $a \in \mathbb{N}$ and for any $i \in \{1, \ldots, n\}$ the function*

$$f(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n) : \mathbb{N}^{n-1} \to \mathbb{N}$$

is computable.

Proof: We begin with showing that the constant functions $g_{n,a} : \mathbb{N}^n \to \mathbb{N}$, $g_{n,a}(x) := a$ are computable for all $n, a \in \mathbb{N}$. The functions $g_{0,a}$ are computable by definition. For $n \geq 0$ we have that $g_{n+1,a}(x_1, \ldots, x_n, 0) = g_{n,a}(x_1, \ldots, x_n)$ and for $x_{n+1} \geq 1$ we have

$$g_{n+1,a}(x_1, \ldots, x_n, x_{n+1}) = \pi_{n+2}(x_1, \ldots, x_n, x_{n+1}, g_{n+1,a}(x_1, \ldots, x_n, x_{n+1} - 1)).$$

Therefore, we have an inductive definition of $g_{n+1,a}$ as in (1.2.2). By induction on n, the function $g_{n,a}$ is computable for all $n, a \in \mathbb{N}$.
Now let f be a computable function $f : \mathbb{N}^n \to \mathbb{N}$ and $a \in \mathbb{N}$. Then the function

$$f(x_1, \ldots, x_{i-1}, a, x_{i+1}, \ldots, x_n) = f(\pi_1(x), \ldots, \pi_{i-1}(x), g_{n,a}(x), \pi_{i+1}(x), \ldots, \pi_n(x))$$

is a composition of computable functions and therefore itself computable. □

Lemma 1.2.4. *The following functions are computable:*

- $f(x, y) = x + y$.
- $f(x, y) = xy$.
- $f(x, y) = x^y$ *(here we set* $0^0 := 1$*).*
- $f(x) = \operatorname{sgn}(x)$.
- $f(x) = \overline{\operatorname{sgn}}(x) := |1 - \operatorname{sgn}(x)|$.
- $f(x, y) = \min\{x, y\}$.
- $f(x, y) = |x - y|$.
- $f(x_1, \ldots, x_n, a, b) = \mu_{a \le y \le b}(R(x_1, \ldots, x_n, y))$ *where* $R(x, y) : \mathbb{N}^{n+1} \to \{0, 1\}$ *is a computable function. The value of* $\mu_{a \le y \le b}(R(x, y))$ *is defined as the smallest* $y \in \mathbb{N}$ *with* $a \le y \le b$ *and* $R(x, y) = 1$*. If there is no such* y*,* $\mu_{a \le y \le b}(R(x, y))$ *is defined as* b*. In particular,* $\mu_{a \le y \le b}(R(x, y)) = b$ *if* $a > b$*.*

Proof: We will introduce three additional functions for the proof. We will also show that these functions are computable.

- Let $f_{2|}(x) := 1$ if $2 \mid x$ and $f_{2|}(x) := 0$ else.
- The predecessor function $pd(0) := 0$ and $pd(x) := x - 1$ for $x \ge 1$.
- The truncated difference $x \dot{-} y := \max\{x - y, 0\}$.

All these functions can now be defined successively by induction as in (1.2.2) in the following way:

$f(x, y) = x + y$	$f_0(x) = x$	$g(x, y, z) = z + 1$
$f(x, y) = xy$	$f_0(x) = 0$	$g(x, y, z) = x + z$
$f(x, y) = x^y$	$f_0(x) = 1$	$g(x, y, z) = xz$
$f(x) = \operatorname{sgn}(x)$	$f_0 = 0$	$g(x, y) = 1$
$f(x) = \overline{\operatorname{sgn}}(x)$	$f_0 = 1$	$g(x, y) = 0$
$f(x) = f_{2\|}(x)$	$f_0 = 1$	$g(x, y) = \overline{\operatorname{sgn}}(y)$
$f(x) = pd(x)$	$f_0 = 0$	$g(x, y) = y + f_{2\|}(x + y)$
$f(x, y) = x \dot{-} y$	$f_0(x) = x$	$g(x, y, z) = pd(z)$
$f(x, y) = \min\{x, y\}$	$f_0(x) = 0$	$g(x, y, z) = z + \operatorname{sgn}(x \dot{-} y)$

Since the functions f_0 and g in the table have always already been proved to be computable or are computable by definition, all functions in the left column are computable.
The function $|x-y|$ is computable since $|x-y| = (x \dot{-} y) + (y \dot{-} x)$.
Finally, let $R' : \mathbb{N}^{n+3} \to \{0,1\}$ be the relation

$$R'(x,a,b,y) := \operatorname{sgn}(\operatorname{sgn}(y \dot{-} b) + (R(x,y) \dot{-} \overline{\operatorname{sgn}}((y+1) \dot{-} a))).$$

Then $R'(x,a,b,y) = 1 \iff y > b \vee (R(x,y) = 1 \wedge y \geq a)$ and this relation is computable (as a function $R' : \mathbb{N}^{n+3} \to \mathbb{N}$) whenever $R(x,y)$ is computable. Also, for all $(x,a,b) \in \mathbb{N}^{n+2}$ there is a $y \in \mathbb{N}$ such that $R'(x,a,b,y) = 1$ (just choose $y > b$). But now we can conclude that $\mu_{a \leq y \leq b}(R(x,y)) = \min\{\mu_y(R'(x,a,b,y)), b\}$ and this function is computable. □

Lemma 1.2.5. *Let $f : \mathbb{N}^2 \to \mathbb{N}$ and $k : \mathbb{N} \to \mathbb{N}$ be computable functions. Then the function $h : \mathbb{N} \to \mathbb{N}$,*

$$h(n) := \prod_{i=0}^{k(n)} f(i,n)$$

is computable.

Proof: We begin with showing that the function $j : \mathbb{N}^2 \to \mathbb{N}$, $j(m,n) := \prod_{i=0}^{n} f(i,m)$ is computable. We can define this function inductively as in (1.2.2) with $f_0(m) := f(0,m)$ and $g(m,n,l) := l \cdot f(n,m)$. These functions are computable by Lemmata 1.2.3 and 1.2.4. Therefore, also j is a computable function. But now we have that $h(n) = j(n,k(n))$ is also a computable function. □

Lemma 1.2.6. (1) *The set of prime numbers is computable.*

(2) *The function $\phi : \mathbb{N} \to \mathbb{N}$, where $\phi(0) := 0$ and $\phi(m) :=$ the mth prime number for $m > 0$, is computable.*

(3) *The function $\rho : \mathbb{N}^2 \to \mathbb{N}$, where $\rho(n,m) :=$ the exponent of the nth prime number in the prime factorization of m for $n, m \geq 1$ and $\rho(n,0), \rho(0,m) := 0$, is computable.*

(4) *The function $\mu : \mathbb{N} \to \mathbb{N}$, where $\mu(m) :=$ the largest prime number dividing m for $m \geq 2$ and $\mu(0), \mu(1) := 0$, is computable.*

(5) *The function $g : \mathbb{N} \to \mathbb{N}$, where $g(m) := 0$ if m is not a prime number and $g(m) := i$ if m is the ith prime number, is computable.*

Proof:

(1) Let $d : \mathbb{N}^2 \to \{0,1\}$ be the relation $d(x,y) = 1 \iff (x > 0 \wedge y > 0 \wedge \exists z \in \mathbb{N} : (z > 0 \wedge xz = y))$. Then d is computable since

$$d(x,y) = \operatorname{sgn}(x) \cdot \operatorname{sgn}(y) \cdot \operatorname{sgn}(y + 1 \dot{-} \mu_{1 \leq z \leq y+1}(\overline{\operatorname{sgn}}(|xz - y|))).$$

We have that $\mathcal{P} = \{x \in \mathbb{N} | x \geq 2, \nexists y \in \mathbb{N} : 1 < y < x, d(y,x) = 1\}$ and

$$\chi_{\mathcal{P}}(n) = \operatorname{sgn}(x \dot{-} 1) \cdot \overline{\operatorname{sgn}}(n \dot{-} \mu_{2 \leq y \leq n}(d(y,n)))$$

is computable.

(2) Let $p : \mathbb{N}^2 \to \{0,1\}$ be the relation $p(x,y) = 1 \iff y \in \mathcal{P} \wedge y > x$. Then we have that

$$p(x,y) = \chi_{\mathcal{P}}(y) \cdot \operatorname{sgn}(y \dot{-} x)$$

is computable and for every $x \in \mathbb{N}$ there is a $y \in \mathbb{N}$ such that $p(x,y) = 1$. We can define ϕ inductively by $\phi(0) := 0$ and $\phi(m+1) := \mu_y(p(\phi(m), y))$.

(3) We claim that $\rho(n,m) = |m - \mu_{0 \leq k \leq m}(d(\phi(n)^{|m-k|}, m))|$ which implies that ρ is a computable function. First we observe that for $m = 0$ we have that

$$|0 - \mu_{0 \leq k \leq 0}(\ldots)| = |0 - 0| = 0 = \rho(0,n)$$

and for $n = 0$ we have that

$$|m - \mu_{0 \leq k \leq m}(d(\phi(0)^{|m-k|}, m))| = |m - \mu_{0 \leq k \leq m}(d(0^{|m-k|}, m))|$$

$$= |m - m| = 0 = \rho(m,0).$$

Now let $n, m > 0$, let $\phi(n) = p$ and $l = \operatorname{ord}_p(m)$. Then we have that

$$|m - \mu_{0 \leq k \leq m}(d(\phi(n)^{|m-k|}, m))| = |m - (m-l)| = l = \rho(n,m).$$

(4) We claim that $\mu(m) = |m - \mu_{0 \leq k \leq m}(\chi_{\mathcal{P}}(m-k) \cdot d(m-k, m))|$ which implies that μ is a computable function. For $m = 0$ we have that

$$|0 - \mu_{0 \leq k \leq 0}(\ldots)| = 0 = \mu(0)$$

and for $m = 1$ we have

$$|1 - \mu_{0 \leq k \leq 1}(\chi_{\mathcal{P}}(1-k) \cdot d(1-k, 1))| = |1 - 1| = 0 = \mu(1).$$

Now let $m \geq 2$ and let p be the largest prime number dividing m. Then we have that

$$|m - \mu_{0 \leq k \leq m}(\chi_{\mathcal{P}}(m-k) \cdot d(m-k, m))| = |m - (m-p)| = p = \mu(m).$$

(5) We have that $g(m) = \chi_{\mathcal{P}}(m)\mu_{1 \leq k \leq m}(\overline{\operatorname{sgn}}(|\phi(k) - m|))$. Therefore, g is computable. □

Remark 1.2.7 (Church-Turing Thesis)**.** In the subsequent chapters we will make use of functions which are in fact computable but for which a formal proof of computability would be too time-consuming. In these cases we will give an informal argument and make use of the Church-Turing thesis, which states that a function is computable if and only if its values can be computed algorithmically (for instance, by a finite-length program running on a computer which has unlimited time and memory), instead. The Church-Turing thesis is discussed in §1.7 of [11].

Closely connected to the notion of computable functions is the notion of computable sets. Informally, a computable set $A \subseteq \mathbb{N}^n$ is a set where we can determine for every $x \in \mathbb{N}^n$ in a finite number of steps if x is an element to A. We will give a definition and some elementary examples of

computable sets.

Definition 1.2.8 (Computable sets)**.** A set $A \subseteq \mathbb{N}^n$ is called computable if its characteristic function $\chi_A : \mathbb{N}^n \to \{0, 1\}$ is computable.

Examples 1.2.9.

- The empty set is computable since the constant function $\chi_\emptyset(x) = 0$ is computable.
- Let $A = \{y_1, \ldots, y_k\} \subseteq \mathbb{N}^n$ be a finite set. Let $y_i = (y_{i,1}, \ldots, y_{i,n})$ for $1 \leq i \leq k$. Then the characteristic function

$$\chi_A(x_1, \ldots, x_n) = \overline{\text{sgn}}\Big(\prod_{i=1}^{k}\sum_{j=1}^{n}|x_j - y_{i,j}|\Big)$$

  is computable by Lemma 1.2.4.

Lemma 1.2.10. *Let $A, B \subseteq \mathbb{N}^n, C \subseteq \mathbb{N}^m$ be computable sets. Then the sets $A \cup B$, $A \cap B$, $A \times C$ and $\mathbb{N}^n \setminus A$ are also computable.*

Proof:

$$\chi_{A\cup B}(x) = \text{sgn}(\chi_A(x) + \chi_B(x)),$$

$$\chi_{A\cap B}(x) = \chi_A(x)\chi_B(x),$$

$$\chi_{A\times C}(x, z) = \chi_A(x)\chi_C(z),$$

$$\chi_{\mathbb{N}^n\setminus A}(x) = \overline{\text{sgn}}(\chi_A(x)).$$

□

A key element in the proof of the negative answer to H10 is the notion of listability. Informally, a set is listable if there is a procedure which generates every element of the set in a finite number of steps. But if we pick an arbitrary element x of a listable set, we usually won't know after how many steps x will be generated.

Definition 1.2.11 (Listable sets)**.** A set $A \subseteq \mathbb{N}^n$ is called listable if A is either empty or the range of some computable function.

The next two theorems will show that the notion of listability is a real generalization of computability.

Theorem 1.2.12. *Every computable set is listable.*

This is Theorem I of §5.1 in [11], p. 58.

Theorem 1.2.13. *There is a listable set that is not computable.*

This is Theorem VI of §5.1 in [11], p. 62-63.

We have now introduced all relevant computational notions for our discussion of Hilbert's tenth problem. But until now, we have formulated the theory of computability only over $\mathbb{N}$. In order to extend it to other algebraic objects than $\mathbb{N}$ (at first to $\mathbb{Z}$ but later on we also want to study H10 over arbitrary rings R) we need to make use of presentations, which will be introduced in the following section.

1.3 Presentations

A presentation of a ring encodes the elements of the ring as non-negative integers. To preserve the structure of the ring we will require the ring-operations to be translated into computable functions.

Definition 1.3.1 (Computability over a ring)**.** Let R be a countable ring and $J : R \to \mathbb{N}$ a map with the following properties:

(1) J is injective.

(2) $J(R) \subseteq \mathbb{N}$ is a computable set.

(3) There are computable functions $J_+, J_-, J_\times : \mathbb{N}^2 \to \mathbb{N}$ such that:
$J_+(J(x), J(y)) = J(x+y)\ \forall x, y \in R$,
$J_-(J(x), J(y)) = J(x-y)\ \forall x, y \in R$,
$J_\times(J(x), J(y)) = J(xy)\ \forall x, y \in R$.

Then R is called a computable ring and J is called a computable presentation of R.
A subset $A \subseteq R^n$ is called computable (listable) if $\bar{J}(A) \subseteq \mathbb{N}^n$ is computable (listable).
A function $f : A \subseteq R^n \to R$ is called computable if there is a computable function $J_f : \mathbb{N}^n \to \mathbb{N}$ such that $J_f(J(x_1), \ldots, J(x_n)) = J(f(x_1, \ldots, x_n))$ for all $(x_1, \ldots, x_n) \in A$.
If R_1 and R_2 are computable rings with computable presentations J_1, J_2, then a function $f : R_1^n \to R_2$ is called computable if there is a computable function $J_f : \mathbb{N}^n \to \mathbb{N}$ with $J_f \circ \bar{J}_1 = J_2 \circ f$.

Definition 1.3.2 (Computable fields)**.** Let K be a countable field. The field K is called a computable field if there is a computable presentation $J : K \to \mathbb{N}$ of K (as a ring) and there is a computable function $J_/ : \mathbb{N}^2 \to \mathbb{N}$ such that

$$J_/(J(x), J(y)) = J\Big(\frac{x}{y}\Big)\ \forall x \in K, y \in K^*.$$

Lemma 1.3.3. *Let R be a computable ring. Then a subset $A \subseteq R^n$ is computable if and only if its characteristic function $\chi_A^R : R^n \to \{0,1\} \subseteq R$ is computable.*

Proof: First note that there are two computable functions $f_1, f_2 : \mathbb{N} \to \mathbb{N}$ fulfilling

$$f_1(0) = J(0_R),\ f_1(1) = J(1_R),\ f_2(J(0_R)) = 0 \text{ and } f_2(J(1_R)) = 1.$$

They can be defined as $f_1(x) = \operatorname{sgn}(x)J(1_R) + \overline{\operatorname{sgn}}(x)J(0_R)$ and $f_2(x) = \operatorname{sgn}(|x - J(0_R)|)$. These functions are computable by Lemma 1.2.4.
Now assume that A is computable. Then the function $\chi_{\bar{J}(A)} : \mathbb{N}^n \to \mathbb{N}$ is computable. We have for all $x \in \mathbb{N}^n$ that

$$J(\chi_A^R(x)) = f_1(\chi_{\bar{J}(A)}(\bar{J}(x))).$$

Therefore, χ_A^R is computable.
On the other hand, suppose that χ_A^R is computable. Then there is a computable function $J_{\chi_A^R} : \mathbb{N}^n \to \mathbb{N}$ such that $J_{\chi_A^R} \circ \bar{J} = J \circ \chi_A^R$. Now we claim that for all $x \in \mathbb{N}^n$ we have that

$$\chi_{\bar{J}(A)}(x) = \chi_{\bar{J}(R^n)}(x) \cdot f_2(J_{\chi_A^R}(x)).$$

Indeed, if $x \notin \bar{J}(R^n)$, then both sides of the equation are zero. On the other hand, if $x \in \bar{J}(R^n)$, we have that

$$\chi_{\bar{J}(A)}(x) = f_2(J(\chi_A^R(\bar{J}^{-1}(x)))) = f_2(J_{\chi_A^R}(x)) = \chi_{\bar{J}(R^n)}(x) \cdot f_2(J_{\chi_A^R}(x))$$

because $\chi_{\bar{J}(R^n)}(x) = 1$. Therefore, $\chi_{\bar{J}(A)}$ is a computable function and A is computable. □

It will be a crucial fact for our discussion of H10 that polynomial functions are computable. Over fields, rational functions are also computable.

Theorem 1.3.4 (Polynomials are computable)**.** *Let R be a computable ring. Then every polynomial $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ is computable.*

Proof: Let f be a polynomial $f \in R[x_1, \ldots, x_n]$. Then f can be built up from basic functions by a finite number of additions and multiplications. More formally, there are functions $f_1, \ldots, f_k : R^n \to R$ such that $f_k = f$ and for every $i \in \{1, \ldots, k\}$, f_i is of one of the following forms:

- $f_i(x_1, \ldots, x_n) = a$ for an $a \in R$.
- $f_i(x_1, \ldots, x_n) = x_j$ for a $j \in \{1, \ldots, n\}$.
- $f_i = f_k + f_l$ for some $k, l < i$.
- $f_i = f_k f_l$ for some $k, l < i$.

We now show that every f_i is computable by induction and in particular f is computable. Let $i \geq 1$ and suppose that $f_1, \ldots, f_{i-1}$ are computable functions.
If $f_i(x_1, \ldots, x_n) = a$ for an $a \in R$, then we define $J_{f_i} : \mathbb{N}^n \to \mathbb{N}$ as $J_{f_i}(x) := J(a)$. The function J_{f_i} is computable (this was shown in the proof of Lemma 1.2.3) and fulfills $J_{f_i} \circ \bar{J} = J \circ f_i$.
If $f_i(x_1, \ldots, x_n) = x_j$, then we define $J_{f_i} : \mathbb{N}^n \to \mathbb{N}$ as $J_{f_i}(x) := \pi_j(x)$. The function J_{f_i} is computable and $J_{f_i} \circ \bar{J} = J \circ f_i$.
If $f_i = f_k + f_l$ for some $k, l < i$, then we define $J_{f_i} : \mathbb{N}^n \to \mathbb{N}$ as $J_{f_i}(x) := J_+(J_{f_k}(x), J_{f_l}(x))$. This function is computable since f_k and f_l are computable and it fulfills

$$J_{f_i}(\bar{J}(x)) = J_+(J_{f_k}(\bar{J}(x)), J_{f_l}(\bar{J}(x))) = J_+(J(f_k(x)), J(f_l(x))) = J(f_k(x) + f_l(x)) = J(f_i(x)).$$

Finally, if $f_i = f_k f_l$ for some $k, l < i$, then we define $J_{f_i} : \mathbb{N}^n \to \mathbb{N}$ as $J_{f_i}(x) := J_\times(J_{f_k}(x), J_{f_l}(x))$ which is computable and fulfills $J_{f_i} \circ \bar{J} = J \circ f_i$ due to the same reason. □

Corollary 1.3.5 (Rational functions are computable)**.** *Let K be a computable field. Then every rational function $f(x_1, \ldots, x_n) \in R(x_1, \ldots, x_n)$ is computable.*

Proof: Let $f = f_1/f_2$ with $f_1, f_2 \in R[x_1, \ldots, x_n]$. Since polynomials are computable by Theorem 1.3.4, there are computable functions $J_{f_1}, J_{f_2} : \mathbb{N}^n \to \mathbb{N}$ with $J \circ f_i = J_{f_i} \circ \bar{J}$ for $i = 1, 2$. Thus, if $x \in R^n$ with $f_2(x) \neq 0$, we have that

$$J(f(x)) = J\left(\frac{f_1(x)}{f_2(x)}\right) = J_/(J(f_1(x)), J(f_2(x))) = J_/(J_{f_1}(\bar{J}(x)), J_{f_2}(\bar{J}(x))).$$

So f is a computable function. □

Our first example of a computable ring will be $\mathbb{Z}$. The next theorem will describe a computable presentation of $\mathbb{Z}$.

Theorem 1.3.6 (A presentation of $\mathbb{Z}$)**.** *Let $J_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{N}$ be defined as*

$$J_{\mathbb{Z}}(n) := \begin{cases} 3^n & n \geq 0 \\ 2 \cdot 3^{-n} & n < 0. \end{cases}$$

Then $J_{\mathbb{Z}}$ is a computable presentation of $\mathbb{Z}$.
Moreover, a subset $A \subseteq \mathbb{N}$ is computable (listable) if and only if $J_{\mathbb{Z}}(A) \subseteq \mathbb{N}$ is computable (listable).

Proof: First of all, the injectivity of $J_{\mathbb{Z}}$ follows from the unique prime factorization for integers. The set $J_{\mathbb{Z}}(\mathbb{Z}) = \{1\} \cup \{2^k 3^n | k \in \{0,1\}, n \geq 1\}$ can be described by computable functions as $J_{\mathbb{Z}}(\mathbb{Z}) = \{1\} \cup \{m \in \mathbb{N} | \rho(1,m) < 2, \mu(m) = 3\}$. Therefore, it is computable by Lemma 1.2.6.
To show that addition is computable we first define the following sets:

$$A_{o,o} := \{(m,n) \in \mathbb{N}^2 : 2 \nmid m, 2 \nmid n\},$$

$$A_{e,e} := \{(m,n) \in \mathbb{N}^2 : 2 \mid m, 2 \mid n\},$$

$$A_{o,e} := \{(m,n) \in \mathbb{N}^2 : 2 \nmid m, 2 \mid n\},$$

$$A_{e,o} := \{(m,n) \in \mathbb{N}^2 : 2 \mid m, 2 \nmid n\},$$

$$A_{o,e,1} := \{(m,n) \in A_{0,e} : 2m \geq n\},$$

$$A_{o,e,2} := \{(m,n) \in A_{0,e} : 2m < n\},$$

$$A_{e,o,1} := \{(m,n) \in A_{e,0} : m > 2n\},$$

$$A_{e,o,2} := \{(m,n) \in A_{e,0} : m \leq 2n\}.$$

These sets are computable by Lemma 1.2.4 and 1.2.6 since $2 \mid m \iff (\rho(1,m) \neq 0 \vee m = 0)$ and $m > n \iff m \dot{-} n \neq 0$.
Now we define a function $f_{o,o} : \mathbb{N}^2 \to \mathbb{N}$, $f_{o,o}(m,n) := 3^{\rho(2,m)+\rho(2,n)}$. This function is computable. Let $x, y \in \mathbb{Z}$ be integers with the property that $x, y \geq 0$. Then we have that $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{o,o}$ and

$$f_{o,o}(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = f_{o,o}(3^x, 3^y) = 3^{x+y} = J_{\mathbb{Z}}(x+y).$$

In a similar way, we define $f_{e,e} : \mathbb{N}^2 \to \mathbb{N}$, $f_{e,e}(m,n) := 2 \cdot 3^{\rho(2,m)+\rho(2,n)}$ and notice that for $x, y \in \mathbb{Z}$ with the property $x, y < 0$ we have that $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{e,e}$ and

$$f_{e,e}(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = f_{e,e}(2 \cdot 3^{-x}, 2 \cdot 3^{-y}) = 2 \cdot 3^{-(x+y)} = J_{\mathbb{Z}}(x+y).$$

Next, we define $f_1 : \mathbb{N}^2 \to \mathbb{N}$, $f_1(m,n) := 3^{|\rho(2,m)-\rho(2,n)|}$. Let $x, y \in \mathbb{Z}$ be integers fulfilling $x \geq 0$, $y < 0$ and $x \geq -y$. Then we have that $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{o,e}$ and since $2J_{\mathbb{Z}}(x) = 2 \cdot 3^x \geq 2 \cdot 3^{-y} = J_{\mathbb{Z}}(y)$ is fulfilled it follows that $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{o,e,1}$. We also have that

$$f_1(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = f_1(3^x, 2 \cdot 3^{-y}) = 3^{|x+y|} = 3^{x+y} = J_{\mathbb{Z}}(x+y).$$

Now let $x, y \in \mathbb{Z}$ be integers with the properties $x < 0$, $y \geq 0$ and $-x \leq y$. Due to the same reasons as above, we have $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{e,o,2}$ and $f_1(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = J_{\mathbb{Z}}(x+y)$.
Lastly, we define $f_2(m,n) := 2 \cdot 3^{|\rho(2,m)-\rho(2,n)|}$. Take $x, y \in \mathbb{Z}$ with $x \geq 0$, $y < 0$ and $x < -y$. Then $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{o,e,2}$ and

$$f_2(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = f_1(3^x, 2 \cdot 3^{-y}) = 2 \cdot 3^{|x+y|} = 2 \cdot 3^{-(x+y)} = J_{\mathbb{Z}}(x+y).$$

Similarly, we have for $x, y \in \mathbb{Z}$ with $x < 0$, $y \geq 0$ and $-x > y$ that $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{e,o,1}$ and $f_2(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = J_{\mathbb{Z}}(x+y)$.
Now we define $J_{\mathbb{Z},+} : \mathbb{N}^2 \to \mathbb{N}$,

$$J_{\mathbb{Z},+}(m,n) := \chi_{A_{o,o}}(m,n) f_{o,o}(m,n) + \chi_{A_{e,e}}(m,n) f_{e,e}(m,n)$$

$$+\chi_{A_{o,e,1} \cup A_{e,o,2}}(m,n) f_1(m,n) + \chi_{A_{o,e,2} \cup A_{e,o,1}}(m,n) f_2(m,n).$$

The function $J_{\mathbb{Z},+} : \mathbb{N}^2 \to \mathbb{N}$ is computable and $J_{\mathbb{Z},+}(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = J_{\mathbb{Z}}(x+y)$ for all $x, y \in \mathbb{Z}$.
To show that subtraction is computable we define a function $g : \mathbb{N} \to \mathbb{N}$,

$$g(x) := \overline{\operatorname{sgn}}(|x-1|) + \operatorname{sgn}(|x-1|)(\rho(1,x) 3^{\rho(2,x)} + \operatorname{sgn}(|1-\rho(1,x)|) 2 \cdot 3^{\rho(2,x)}).$$

The function g is computable. It fulfills

$$g(J_{\mathbb{Z}}(n)) = \begin{cases} 1 & n = 0 \\ 2 \cdot 3^n & n > 0 \\ 3^{-n} & n < 0. \end{cases}$$

So we have that $J_{\mathbb{Z}}(-x) = (g \circ J_{\mathbb{Z}})(x)$ for all $x \in \mathbb{Z}$ and we can define $J_{\mathbb{Z},-}(m,n) := J_{\mathbb{Z},+}(m, g(n))$. This function is computable and fulfills $J_{\mathbb{Z},-}(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = J_{\mathbb{Z}}(x-y)$ for all $x, y \in \mathbb{Z}$.
Considering multiplication, we define functions $h_1, h_2 : \mathbb{N}^2 \to \mathbb{N}$, $h_1(m,n) := 3^{\rho(2,m)\rho(2,n)}$ and $h_2(m,n) := 2 \cdot 3^{\rho(2,m)\rho(2,n)}$. If $x, y \in \mathbb{Z}$ with $x, y \geq 0$, then we have that $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{o,o}$ and

$$h_1(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = h_1(3^x, 3^y) = 3^{xy} = J_{\mathbb{Z}}(xy).$$

If $x, y \in \mathbb{Z}$ and $x, y < 0$, then $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{e,e}$ and

$$h_1(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = h_1(2 \cdot 3^{-x}, 2 \cdot 3^{-y}) = 3^{(-x)(-y)} = 3^{xy} = J_{\mathbb{Z}}(xy).$$

If $x, y \in \mathbb{Z}$ with $x \geq 0$ and $y < 0$, then $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{o,e}$ and

$$h_2(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = h_2(3^x, 2 \cdot 3^{-y}) = 2 \cdot 3^{x(-y)} = 2 \cdot 3^{-(xy)} = J_{\mathbb{Z}}(xy).$$

Finally, if $x, y \in \mathbb{Z}$ with $x < 0$ and $y \geq 0$, then $(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) \in A_{e,o}$ and $h_2(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = J_{\mathbb{Z}}(xy)$ due to the same reason.
Now we define $J_{\mathbb{Z},\times} : \mathbb{N}^2 \to \mathbb{N}$,

$$J_{\mathbb{Z},\times}(m,n) := \chi_{A_{o,o} \cup A_{e,e}}(m,n) h_1(m,n) + \chi_{A_{o,e} \cup A_{e,o}}(m,n) h_2(m,n).$$

The function $J_{\mathbb{Z},\times}$ is computable since h_1 and h_2 are computable. Due to the calculation above we have that $J_{\mathbb{Z},\times}(J_{\mathbb{Z}}(x), J_{\mathbb{Z}}(y)) = J_{\mathbb{Z}}(xy)$ for all $x, y \in \mathbb{Z}$. Thus, we have shown that $J_{\mathbb{Z}}$ is a computable presentation of $\mathbb{Z}$ and, in particular, that $\mathbb{Z}$ is a computable ring.
The set $J_{\mathbb{Z}}(\mathbb{N})$ is computable since $J_{\mathbb{Z}}(\mathbb{N}) = \{1\} \cup \{m \in \mathbb{N} | \rho(1, m) = 0, \mu(m) = 3\}$. Now let $A \subseteq \mathbb{N}$. Suppose that A is a computable set. Then $\chi_{J_{\mathbb{Z}}(A)}(n) = \chi_{J_{\mathbb{Z}}(\mathbb{N})}(n)\chi_A(\rho(2, n))$ is a computable function. Therefore, $J_{\mathbb{Z}}(A)$ is computable.
Conversely, suppose that $J_{\mathbb{Z}}(A)$ is computable. Then $\chi_A(n) = \chi_{J_{\mathbb{Z}}(A)}(3^n)$ is a computable function by Lemma 1.2.4.
Now suppose that A is a listable set. Thus, there is a computable function $f : \mathbb{N} \to \mathbb{N}$ such that $f(\mathbb{N}) = A$. The function $e_3 : \mathbb{N} \to \mathbb{N}$, $e_3(n) := 3^n$ is computable and $(e_3 \circ f)(\mathbb{N}) = J_{\mathbb{Z}}(A)$. This proves that $J_{\mathbb{Z}}(A)$ is listable.
Lastly, suppose that $J_{\mathbb{Z}}(A)$ is listable. Let $f : \mathbb{N} \to \mathbb{N}$ be a computable function such that $f(\mathbb{N}) = J_{\mathbb{Z}}(A)$. Then the function $l_3 : \mathbb{N} \to \mathbb{N}$, $l_3(n) := \rho(2, n)$ is computable and $A = (l_3 \circ f)(\mathbb{N})$. Thus, A is a listable set. □

Up to this point we cannot be sure if there are different presentations of $\mathbb{Z}$ which are not equivalent. A function $f : \mathbb{Z}^n \to \mathbb{Z}$ could be computable under one presentation and not computable under another presentation. Luckily, we have the following result for finitely generated rings and fields:

Theorem 1.3.7 (Equivalence of presentations)**.** *Let R be either a computable finitely generated ring or a computable finite field extension of $\mathbb{Q}$. If $J_1, J_2 : R \to \mathbb{N}$ are two computable presentations of R, then there is a computable function $f_{1,2} : \mathbb{N} \to \mathbb{N}$ such that $f_{1,2} \circ J_1 = J_2$.*

This is Proposition A.6.5 of [15], p. 230-231.

Now that we have ensured that all computable presentations of $\mathbb{Z}$ are essentially equivalent, we can focus on the answer to H10.

1.4 Diophantine sets and the negative answer to H10

We will begin with introducing the notion of diophantine sets. Diophantine sets will not only be of essential importance in the proof of the negative answer to H10, but also in the later chapters when we investigate the problem over other rings than $\mathbb{Z}$.

Definition 1.4.1 (Diophantine sets, diophantine definition)**.** Let R be a ring. A subset $A \subseteq R^n$ is called diophantine (over R) if there is a $m \geq 0$ and a polynomial $f \in R[x_1, \ldots, x_n, y_1, \ldots, y_m]$ such that

$$A = \{x \in R^n | \exists y \in R^m : f(x, y) = 0\}.$$

We call f a diophantine definition of A over R.

Using the terminology of algebraic geometry, we could describe diophantine sets as projections of affine varieties which are defined by a single polynomial. If A and f are defined as above, $\pi_{1,\ldots,n} : R^{n+m} \to R^n$ is the projection onto the first n variables and $V(f) := \{x \in R^{n+m} | f(x) = 0\}$, then $A = \pi_{1,\ldots,n}(V(f))$.

Examples 1.4.2. Let the R be a ring. Then the following sets are all diophantine:

(1) $R = \{x \in R | 0 = 0\}$.

(2) $\emptyset = \{x \in R | 1 = 0\}$.

(3) $\{a\} = \{x \in R | x - a = 0\}$ for any $a \in R$.

(4) $\{a_1, \ldots, a_n\} = \{x \in R | (x - a_1) \cdots (x - a_n) = 0\}$ with $a_1, \ldots a_n \in R$.

(5) $R^* = \{x \in R | \exists y \in R : xy - 1 = 0\}$.

Notice that $R^* = \{x \in R | x \neq 0\}$ if R is a field. Thus, we have found a diophantine definition for inequalities. However, if R is an arbitrary ring, it is not at all clear how to define inequalities. For $\mathbb{Z}$ we have the following (see Theorem 2.3.5 for a proof):

(6) $\mathbb{Z} \setminus \{0\} = \{x \in \mathbb{Z} | \exists a, b, c \in \mathbb{Z} : ax - (2b - 1)(3c - 1) = 0\}$.

(7) $\{x \in \mathbb{Z} | x \geq a\} = \{x \in \mathbb{Z} | \exists y_1, y_2, y_3, y_4 \in \mathbb{Z} : (x - a) - (y_1^2 + y_2^2 + y_3^2 + y_4^2) = 0\}$ and
$\{x \in \mathbb{Z} | x \leq a\} = \{x \in \mathbb{Z} | \exists y_1, y_2, y_3, y_4 \in \mathbb{Z} : (a - x) - (y_1^2 + y_2^2 + y_3^2 + y_4^2) = 0\}$ for any $a \in \mathbb{Z}$.

We can define inequalities over $\mathbb{Q}$ in the same way.

The following theorem was the decisive step in proving the negative answer to Hilbert's tenth problem. It was first proved by Yuri Matiyasevich in 1970, heavily building on previous works of Martin Davis, Hilary Putnam and Julia Robinson.

Theorem 1.4.3 (Matiyasevich)**.** *Let $A \subseteq \mathbb{Z}$. Then A is diophantine if and only if A is listable.*

A proof of this theorem can be found in [7].
Now we can finally state the main theorem of this chapter:

Theorem 1.4.4 (H10 is undecidable)**.** *There is no computable map $T : \bigcup_{n \geq 1} \mathbb{Z}^n \to \{0, 1\}$ such that $T(t) = 1$ if and only if the following conditions are fulfilled:*

- *There is a $m \geq 1$ and a $f \in \mathbb{Z}[x_1, \ldots, x_m]$ such that $C_{\mathbb{Z}}(f) = t$.*
- *There is a $x \in \mathbb{Z}^m$ with $f(x) = 0$.*

Proof: Suppose that such a T exists. Then, by Definition 1.3.1, there is a computable function $J_T : \bigcup_{n \geq 1} \mathbb{N}^n \to \mathbb{N}$ with $J_T(\bar{J}(x)) = J(T(x))$ for all $x \in \mathbb{Z}$.
Now let $A \subseteq \mathbb{N}$ be a listable set that is not computable (such a set exists by Theorem 1.2.13). By Theorem 1.3.6, A is also listable as a subset of $\mathbb{Z}$. Now Theorem 1.4.3 tells us that A is diophantine. Thus, there is a $n \geq 0$ and a polynomial $f \in \mathbb{Z}[x, y_1, \ldots, y_n]$ of degree $d \geq 0$,

$$f(x, y_1, \ldots, y_n) = \sum_{0 \leq i, j_1, \ldots, j_n \leq d} a_{i, j_1, \ldots, j_n} x^i y_1^{j_1} \cdots y_n^{j_n}$$

such that

$$A = \{x \in \mathbb{Z} | \exists y \in \mathbb{Z}^n : f(x, y) = 0\}. \tag{1.4.1}$$

If we fix any $x_0 \in \mathbb{Z}$, we get a polynomial $f(x_0, y) \in \mathbb{Z}[y_1, \ldots, y_n]$ of the form

$$\sum_{0 \leq i, j_1, \ldots, j_n \leq d} a_{i,j_1,\ldots,j_n} x_0^i y_1^{j_1} \cdots y_n^{j_n} = \sum_{0 \leq j_1, \ldots, j_n \leq d} \left(\sum_{1 \leq i \leq d} a_{i,j_1,\ldots,j_n} x_0^i \right) y_1^{j_1} \cdots y_n^{j_n}$$

$$= \sum_{0 \leq j_1, \ldots, j_n \leq d} f_{j_1,\ldots,j_n}(x_0) y^{j_1} \cdots y^{j_n}$$

where $f_{j_1,\ldots,j_n} \in \mathbb{Z}[x]$. Since polynomials are computable (Theorem 1.3.4), there are computable functions $J_{f_{j_1,\ldots,j_n}} : \mathbb{N} \to \mathbb{N}$ such that $J_{f_{j_1,\ldots,j_n}} \circ J = J \circ f_{j_1,\ldots,j_n}$.
Because of (1.4.1), we have that

$$\chi_A^{\mathbb{Z}}(x_0) = T(C_{\mathbb{Z}}(f(x_0, y))) = T(d, n, f_{j_1,\ldots,j_n}(x_0), 0 \leq j_1, \ldots, j_n \leq d).$$

If we apply J to both sides of this equation, we get:

$$J(\chi_A^{\mathbb{Z}}(x_0)) = J_T(J(d), J(n), J_{f_{j_1,\ldots,j_n}}(J(x_0)), 0 \leq j_1, \ldots, j_n \leq d).$$

Since the composition of computable functions is computable and because of Lemma 1.2.3, the right side of the last equation is a computable function in $J(x_0)$. So we have found a computable function

$$J_{\chi_A^{\mathbb{Z}}}(m) := J_T(J(d), J(n), J_{f_{j_1,\ldots,j_n}}(m), 1 \leq j_1, \ldots, j_n \leq n)$$

with $J_{\chi_A^{\mathbb{Z}}} \circ J = J \circ \chi_A^{\mathbb{Z}}$. Thus, $\chi_A^{\mathbb{Z}}$ is a computable function and it follows with Lemma 1.3.3 that A is a computable subset of $\mathbb{Z}$. With Theorem 1.3.6 we can finally conclude that A is also a computable subset of $\mathbb{N}$ - a contradiction to our assumption. □

2 H10 over computable rings

2.1 Formulation of the problem and ways to solve it

If we generalize the posed question in Hilbert's tenth problem by not only considering polynomials over $\mathbb{Z}$ but over any ring, we obtain a whole new class of problems. Of course we should only consider rings over which it makes sense to speak of computability, that is, computable rings.
The content of this chapter, as well as related topics, is discussed in chapter 3 of [15].
For a given computable ring R with a computable presentation J we will again fix a way of encoding polynomials over R. We define a map

$$C_{R,J} : \bigcup_{n,m\geq 0} R[x_1,\ldots,x_n,y_1\ldots,y_m] \to \bigcup_{n\geq 1} \mathbb{N}^n,$$

$$C_{R,J}\Big(\sum_{0\leq i_1,\ldots,i_n,j_1\ldots,j_m\leq d} a_{i_1,\ldots,i_n,j_1,\ldots,j_m} x_1^{i_1}\cdots x_n^{i_n} y_1^{j_1}\cdots y_m^{j_m}\Big)$$
$$:= (d,n,m,J(a_{i_1,\ldots,i_n,j_1,\ldots,j_m}), 0\leq i_1,\ldots,i_n,j_1\ldots,j_m\leq d)$$

where the $J(a_{i_1,\ldots,i_n,j_1,\ldots,j_m})$ are arranged in lexicographic order.
A convenient way to formulate H10 over R (as found in [15], p. 37-38) is the following:

Definition 2.1.1 (H10 over a ring R)**.** Let R be a computable ring and J a computable presentation of R. We say that H10 is decidable over R under J if there is a computable function $T_R : \bigcup_{k\geq 1}\mathbb{N}^k \to \{0,1\}$ such that $T_R(t,u) = 1$ if and only if the following conditions are fulfilled:

- There are $n,m\geq 0$ and a $f\in R[x_1,\ldots,x_n,y_1,\ldots,y_m]$ with $C_{R,J}(f) = t$.
- There is a $x\in R^n$ such that $\bar{J}(x) = u$.
- There is a $y\in R^m$ with $f(x,y) = 0$.

Otherwise, we say that H10 is undecidable over R under J.

We proved that H10 is undecidable over $\mathbb{Z}$ by finding a diophantine set that is not computable. The following theorem will make clear that the existence of such a set always implies undecidability of H10.

Theorem 2.1.2. *If H10 is decidable over a computable ring R under a presentation J, then every diophantine subset $A\subseteq R^n$ is computable under J.*

Proof: Let $A = \{x\in R^n | \exists y\in R^m : f(x,y) = 0\}$ for some polynomial $f\in R[x_1,\ldots,x_n,y_1,\ldots,y_m]$. Then we have that $\chi_A(x) = T_R(C_{R,J}(f),\bar{J}(x))$ for all $x\in R^n$. This implies the identity $\chi_{\bar{J}(A)}(x) = \chi_{\bar{J}(R^n)}(x)T_R(C_{R,J}(f),x)$ for all $x\in\mathbb{N}^n$. But this is a computable function by the Lemmata 1.2.3, 1.2.4. Therefore, A is computable. □

It follows that H10 is undecidable over $\mathbb{Z}$ under any computable presentation in accordance with Definition 2.1.1. It would be convenient if there was a way to use this fact to prove undecidability of H10 over other rings or, more generally, to use undecidability of H10 over one ring to establish undecidability over another ring.
A practical instrument to do so is the *diophantine model*:

Definition 2.1.3 (Diophantine model)**.** Let R_1, R_2 be two computable rings and $\Phi : R_1 \to R_2^n$, $\Phi = (\Phi_1, \dots, \Phi_n)$ a map with the following properties:

(1) For every diophantine set $A \subseteq R_1^k$ there is a diophantine set $\tilde{A} \subseteq R_2^{nk}$ such that $\bar{\Phi}(A) \subseteq \tilde{A}$ and $\bar{\Phi}(R_1^k \setminus A) \cap \tilde{A} = \emptyset$.

(2) There are computable presentations $J_1 : R_1 \to \mathbb{N}$ and $J_2 : R_2 \to \mathbb{N}$ such that the maps $J_2 \circ \Phi_i \circ J_1^{-1} : J_1(R_1) \to J_2(R_2)$ are restrictions of computable functions $\phi_i : \mathbb{N} \to \mathbb{N}$ for all $i \in \{1, \dots, n\}$.

Then we will say that R_2 has a diophantine model of R_1.
The diophantine model is called *tight* if $\bar{\Phi}(A) \subseteq R_2^{kn}$ is a diophantine set for every diophantine set $A \subseteq R_1^k$.

Lemma 2.1.4 (Diophantine models are injective)**.** *Let R_1, R_2 be two computable rings such that R_2 has a diophantine model of R_1. Then Φ (defined as in Definition 2.1.3) is injective.*

Proof Let $x, y \in R_1$ with $x \neq y$. Since $\{x\}$ is a diophantine set, there is a diophantine set $D \subseteq R_2^n$ such that $\Phi(\{x\}) \subseteq D$ and $\Phi(R_1 \setminus \{x\}) \cap D = \emptyset$. Since $y \in R_1 \setminus \{x\}$, we have that $\Phi(\{y\}) \cap D = \emptyset$. But this implies that $\Phi(x) \neq \Phi(y)$. □

The next theorem will show how diophantine models can be used to convey undecidability of H10 from one ring to another.

Theorem 2.1.5. *Let R_1, R_2 be two computable rings such that R_2 has a diophantine model $\Phi : R_1 \to R_2^n$ of R_1 under some presentations J_1 of R_1 and J_2 of R_2. Suppose that one of the following statements is true:*

(1) *H10 is undecidable over R_1 under J_1 and there is a computable function $F : \bigcup_{i\geq 1} \mathbb{N}^i \to \bigcup_{i\geq 1} \mathbb{N}^i$ such that for every diophantine set $A \subseteq R_1^k$ with defining polynomial $f \in R[x_1, \dots, x_k, y_1 \dots y_l]$ there is a diophantine set $\tilde{A} \subseteq R_2^{nk}$ as in Definition 2.1.3 with defining polynomial $g \in R[x_1, \dots, x_{nk}, y_1 \dots y_m]$ that fulfills $F(C_{R_1,J_1}(f)) = C_{R_2,J_2}(g)$.*

(2) *There is a diophantine subset $A \subseteq R_1^k$ that is not computable under J_1 (therefore, H10 is undecidable over R_1 under J_1).*

Then H10 is undecidable over R_2 under J_2.

Proof: We notice beforehand that there is a computable function $\phi : \mathbb{N} \to \mathbb{N}^n$ such that $\phi(x) = (\bar{J}_2 \circ \Phi \circ J_1^{-1})(x)$ for all $x \in J_1(R_1)$.
Suppose that statement (1) is true, but H10 is decidable over R_2 under J_2. Then there is a computable function $T_{R_2} : \bigcup_{n\geq 1} \mathbb{N}^n \to \{0, 1\}$ as in Definition 2.1.1. Now write $A(f)$ for a diophantine set

over R_1 with defining polynomial f and $\tilde{A}(g)$ for a diophantine set over R_2 with defining polynomial g. Then we have that

$$x \in A(f) \iff \Phi(x) \in \tilde{A}(C_{R_2,J_2}^{-1} \circ F \circ C_{R_1,J_1}(f)) \tag{2.1.1}$$

for all $x \in R^k$ and $f \in R[x_1, \ldots, x_k, y_1, \ldots, y_l]$. We now want to construct a computable function $T : \bigcup_{i \geq 1} \mathbb{N}^i \to \{0,1\}$ fulfilling the requirements of Definition 2.1.1 for R_1 under J_1.
Let $x \in \mathbb{N}^i$ with $i \geq 1$. We want to set $T(x) = 0$ if there is are no $k, l \in \mathbb{N}$, $f \in R[x_1, \ldots, x_k, y_1, \ldots, y_l]$ and $x \in R^k$ such that $x = (C_{R_1,J_1}(g), \bar{J}_1(x))$. Therefore, we let $T(x) = 0$ if x is not of the form $x = (d, k, l, t, u)$ with $d, k, l \in \mathbb{N}$, $t \in \mathbb{N}^h$ where $h = \sum_{j=0}^{d}(k+l)^j$ and $u \in \mathbb{N}^k$. Otherwise, we have that $C_{R_1,J_1}^{-1}(d, k, l, t) \in R_1[x_1, \ldots, x_n]$ if $t \in \bar{J}_1(R_1^h)$. So we define

$$T(d, k, l, t, u) := \chi_{\bar{J}_1(R_1^h)}(t) \cdot \chi_{\bar{J}_1(R_1^k)}(u) \cdot T_{R_2}(F(d, k, l, t), \bar{\phi}(u)).$$

It follows from (2.1.1) that T meets the requirements. Since T is a computable function, this is a contradiction to our assumption that H10 is undecidable over R_1 under J_1.
Now suppose that statement (2) is true. Let $A \subseteq R_1^k$ be a diophantine subset which is not computable under J_1. Let $\tilde{A} \subseteq R_2^{nk}$ be a diophantine set fulfilling $\bar{\Phi}(A) \subseteq \tilde{A}$ and $\bar{\Phi}(R_1^k \setminus A) \cap \tilde{A} = \emptyset$. Then we have that

$$\chi_A(x) = (\chi_{\tilde{A}} \circ \Phi)(x) \; \forall x \in R_1^k.$$

We now claim that

$$\chi_{\bar{J}_1(A)}(x) = \chi_{\bar{J}_1(R^k)}(x) \cdot (\chi_{\bar{J}_2(\tilde{A})} \circ \phi)(x). \tag{2.1.2}$$

Indeed, suppose that $x \in \bar{J}_1(R^k)$. Since $\chi_{\bar{J}_1(R^k)}(x) = 1$ we have that

$$\chi_{\bar{J}_1(A)}(x) = \chi_A({\bar{J}_1}^{-1}(x)) = (\chi_{\tilde{A}} \circ \Phi)({\bar{J}_1}^{-1}(x)) = (\chi_{\tilde{A}} \circ {\bar{J}_2}^{-1}) \circ (\bar{J}_2 \circ \Phi \circ {\bar{J}_1}^{-1})(x)$$

$$= (\chi_{\bar{J}_2(\tilde{A})} \circ \phi)(x) = \chi_{\bar{J}_1(R^k)}(x) \cdot (\chi_{\bar{J}_2(\tilde{A})} \circ \phi)(x).$$

On the other hand, if $x \notin \bar{J}_1(R^k)$, then both sides of (2.1.2) are zero. Since $\tilde{A}$ is computable under J_2 by Theorem 2.1.2, the function $\chi_{\bar{J}_2(\tilde{A})}$ is computable. With Lemma 1.2.4 it follows that $\chi_{\bar{J}_1(A)}$ is computable. This yields a contradiction to our assumption that A is not computable under J_1. □

Notice, that when we utilize diophantine models of $\mathbb{Z}$, statement (2) of Theorem 2.1.5 is true. So we can be sure that H10 is undecidable over every ring that has a diophantine model of $\mathbb{Z}$.
If we have two rings $R_1 \subseteq R_2$ with certain properties such that R_1 has a diophantine definition over R_2 and H10 is undecidable over R_1, H10 is also undecidable over R_2. Before we prove this fact, we will establish a Lemma which is very useful when working with diophantine sets.

Lemma 2.1.6. *Let R be a ring whose quotient field K is not algebraically closed and let $f_1, \ldots, f_k \in R[x_1, \ldots, x_n]$ be polynomials over R. Then there is a polynomial $g \in R[x_1, \ldots, x_n]$ which fulfills*

$$f_1(x) = \ldots = f_k(x) = 0 \iff g(x) = 0.$$

Also, there is a constructive and uniform (in R) way to compute the coefficients of g from the coefficients of $f_1, \ldots, f_k$ (in other words, for a computable presentation J of R there is a computable function which maps $(k, C_{R,J}(f_1), \ldots, C_{R,J}(f_k))$ onto $C_{R,J}(g)$).

Proof: It suffices to proof the lemma for $k = 2$. Let $h \in K[x]$ be a non-constant polynomial with no roots in K. We can assume that $h(x) = a_0 + a_1 x + \ldots + a_m x^m$ with $a_i \in R$ and $a_m \neq 0$. We also notice that

$$\tilde{h}(x) := x^m h(1/x) = a_m + a_{m-1} x + \ldots + a_0 x^m$$

is another polynomials with no roots in K. (If $\tilde{h}(x) = 0$ for some $x \neq 0$, it would follow that $h(1/x) = 0$. Further, $\tilde{h}(0) = a_m \neq 0$.)
Now we define

$$g(x) := \sum_{i=0}^{m} a_i f_1(x)^i f_2(x)^{m-i}.$$

Of course, $g \in R[x_1, \ldots, x_n]$. If $x \in R^n$ fulfills $f_1(x) = f_2(x) = 0$, it is clear that also $g(x) = 0$.
On the other hand, suppose that $g(x) = 0$ for some $x \in R^n$. If $f_1(x) \neq 0$, it would follow that $\tilde{h}(f_2(x)/f_1(x)) = 0$ and $f_2(x) \neq 0$ would imply that $h(f_1(x)/f_2(x)) = 0$. So we have that $f_1(x) = f_2(x) = 0$.
Finally, note that since we have given an explicit definition for g which only depends on the a_i (which can be fixed for R) and the polynomials f_1, f_2, our second assertion is also true. □

Example 2.1.7. Let $f_1, \ldots, f_k \in \mathbb{Z}[x_1, \ldots, x_n]$ be a finite number of polynomials over $\mathbb{Z}$. Then

$$f_1(x) = \ldots = f_k(x) = 0 \iff f_1(x)^2 + \ldots + f_k(x)^2 = 0.$$

(Here, the polynomial without roots we use is $x^2 + 1 \in \mathbb{Z}[x]$.)

Lemma 2.1.6 has the following corollary:

Lemma 2.1.8. *Let R be a ring whose quotient field is not algebraically closed. Then all finite unions, intersections and Cartesian products of diophantine sets are again diophatine.*

Proof: Let $A, B \subseteq R^n$, $C \subseteq R^k$ be diophantine sets with defining polynomials

$$f, g \in R[x_1, \ldots, x_n, y_1, \ldots, y_m],\ h \in R[x_1, \ldots, x_k, y_1, \ldots, y_l].$$

Then we have that

$$A \cup B = \{x \in R^n | \exists y \in R^m : f(x, y) g(x, y) = 0\},$$

$$A \cap B = \{x \in R^n | \exists y_1, y_2 \in R^m : f(x, y_1) = g(x, y_2) = 0\},$$

$$A \times C = \{(x, z) \in R^{n+k} | \exists (y, w) \in R^{m+l} : f(x, y) = h(z, w) = 0\}.$$

These sets are diophantine by Lemma 2.1.6. □

Theorem 2.1.9 (Lifting undecidability of H10 from subring to superring)**.** *Let R_1, R_2 be two computable rings such that $R_1 \subseteq R_2$. Suppose that the following requirements are fulfilled:*

- *R_1 has a diophantine definition over R_2.*
- *The quotient field of R_2 is not algebraically closed.*
- *There is a computable presentation J_2 of R_2 that is the extension of a computable presentation J_1 of R_1 (which is equivalent to requiring $J_2(R_1)$ to be computable).*

- *H10 is undecidable over R_1 under J_1.*

Then H10 is undecidable over R_2 under J_2.

Proof: We will show that R_2 has a diophantine model of R_1 (with Φ the inclusion $R_1 \hookrightarrow R_2$) fulfilling requirement (1) of Theorem 2.1.5.
Notice that requirement (2) of Definition 2.1.3 is obviously fulfilled since $J_2 \circ \Phi \circ J_1^{-1}$ is the identity on $J_1(R_1)$.
There is a $f \in R_2[x, y_1, ..., y_n]$ such that

$$R_1 = \{x \in R_2 | \exists y \in R_2^n : f(x, y) = 0\}.$$

Now let $A \subseteq R_1^k$ be a diophantine subset

$$A = \{x \in R_1^k | \exists y \in R_1^m : g(x, y) = 0\}$$

for a polynomial $g \in R_1[x_1, \ldots, x_k, y_1, \ldots, y_m]$. Combining the two definitions, we derive

$$A = \{x = (x_1, \ldots, x_k) \in R_2^k | \exists y = (y_1, \ldots, y_m) \in R_2^m, \exists z_1, \ldots, z_k, u_1, \ldots, u_m \in R_2^n :$$

$$g(x, y) = f(x_1, z_1) = \ldots = f(x_k, z_k) = f(y_1, u_1) = \ldots = f(y_m, u_m) = 0\}.$$

Since the quotient field of R_2 is not algebraically closed, Lemma 2.1.6 assures us that there is a polynomial $h \in R_2[x_1, \ldots, x_k, y_1, \ldots, y_m, z_{1,1}, \ldots, z_{k,n}, u_{1,1}, \ldots, u_{m,n}]$ with

$$h(x, y, z, u) = 0 \iff g(x, y) = f(x_i, z_i) = f(y_j, u_j) = 0 \text{ with } 1 \leq i \leq k, 1 \leq j \leq m.$$

Thus, we have found a diophantine definition of A over R_2:

$$A = \{x \in R_2^k | \exists y \in R_2^{n(m+k)+m} : h(x, y) = 0\}.$$

Finally, we observe that our construction of h from g is computable and uniform by Lemma 2.1.6 and the fact that f can be fixed for R_1, R_2. □

Before finishing this section, we will establish a handy criterion which allows us to show that a ring has a diophantine model of $\mathbb{Z}$ without checking for every diophantine set over $\mathbb{Z}$ that there is a diophantine set which contains its image and is disjoint with the image of its complement. As a preparation, we will prove that all diophantine sets are listable even if H10 is undecidable over the given ring.

Lemma 2.1.10 (Diophantine sets are listable)**.** *Let R be a computable ring with a computable presentation $J : R \to \mathbb{N}$. If $A \subseteq R^n$ is a diophantine set, the set $\bar{J}(A) \subseteq \mathbb{N}^n$ is listable.*

Proof: There is a polynomial $f \in R[x_1, \ldots, x_n, y_1, \ldots, y_m]$ such that

$$A = \{x \in R^n | \exists y \in R^m : f(x, y) = 0\}.$$

Since polynomials are computable by Theorem 1.3.4, there is computable function $J_f : \mathbb{N}^n \to \mathbb{N}$ with $J \circ f = J_f \circ \bar{J}$. Thus,

$$\bar{J}(A) = \{\bar{J}(x) | x \in R^n, \exists y \in R^m : f(x,y) = 0\} = \{u \in \bar{J}(R^n) | \exists v \in \bar{J}(R^m) : J_f(u,v) = J(0)\}.$$

Since the set $\bar{J}(R^{n+m}) = J(R)^{n+m}$ is computable by Lemma 1.2.10, it is in consequence also listable by Theorem 1.2.12. Let $s : \mathbb{N} \to \mathbb{N}^{n+m}$ be a computable function with $s(\mathbb{N}) = \bar{J}(R^{n+m})$. Without loss of generality, we can assume that $A \neq \emptyset$. Let $w \in \bar{J}(A)$. Now define a function $t : \mathbb{N} \to \mathbb{N}^n$ by

$$t(k) := \overline{\operatorname{sgn}}(|J_f(s(k)) - J(0)|) \cdot (\pi_1(s(k)), \ldots, \pi_n(s(k))) + \operatorname{sgn}(|J_f(s(k)) - J(0)|) \cdot w.$$

The function t is computable and $t(\mathbb{N}) = \bar{J}(A)$ since $t(k) = u$ if $s(k) = (u,v)$ with $J_f(u,v) = J(0)$ and $t(k) = w$ else. □

Theorem 2.1.11 (Diophantine models of $\mathbb{Z}$)**.** *Let R be a computable ring whose quotient field is not algebraically closed. If there is an injective map $\tau : \mathbb{Z} \to R^k$ for which the two sets*

$$D_+ := \{(\tau(x), \tau(y), \tau(x+y)) | x, y \in \mathbb{Z}\} \subseteq R^{3k},$$

$$D_\times := \{(\tau(x), \tau(y), \tau(xy)) | x, y \in \mathbb{Z}\} \subseteq R^{3k}$$

are diophantine over R, the ring R has a tight diophantine model of $\mathbb{Z}$ and H10 is undecidable over R (under any computable presentation of R).

Proof: Beforehand, we notice that the set $\tau(\mathbb{Z}) \subseteq R^k$ is diophantine since it is the projection of D_+ onto the first k variables. Also, by assumption there is a $l \in \mathbb{N}$ and there are two polynomials $f_+, f_\times \in R[u_1, \ldots, u_{3k}, v_1, \ldots, v_l]$ such that

$$x + y = z \iff \exists v \in R^l : f_+(\tau(x), \tau(y), \tau(z), v) = 0 \ \forall x, y, z \in \mathbb{Z},$$

$$xy = z \iff \exists v \in R^l : f_\times(\tau(x), \tau(y), \tau(z), v) = 0 \ \forall x, y, z \in \mathbb{Z}.$$

We now want to prove the following assertion:
For every $f \in \mathbb{Z}[x_1, \ldots, x_n]$ there is a $m \in \mathbb{N}$ and a $g \in R[u_1, \ldots, u_{kn}, v_1, \ldots, v_k, w_1, \ldots, w_m]$ such that

$$f(x) = y \iff \exists w \in R^m : g(\bar{\tau}(x), \tau(y), w) = 0 \ \forall x, y \in \mathbb{Z}.$$

Let $f \in \mathbb{Z}[x_1, \ldots, x_n]$. We already noticed in the proof of Theorem 1.3.4 that there are polynomials $f_1, \ldots, f_i \in \mathbb{Z}[x_1, \ldots, x_n]$ such that $f_i = f$ and for every $j \in \{1, \ldots, i\}$ the polynomial f_j is of one of the following forms:

(1) $f_j(x_1, \ldots, x_n) = a$ for an $a \in \mathbb{Z}$,

(2) $f_j(x_1, \ldots, x_n) = x_{i_0}$ for an $i_0 \in \{1, \ldots, n\}$,

(3) $f_j = f_s + f_t$ for some $s, t < j$,

(4) $f_j = f_s f_t$ for some $s, t < i$.

Now let $j \in \{1, \dots, i\}$ and assume that the assertion is already proved for f_s with $s < j$.
Let f_j be defined as in (1). Then $f_j(x) = y \iff \tau(y) - \tau(a) = 0$.
Let f_j be defined as in (2). Then $f_j(x) = y \iff \tau(x_{i_0}) - \tau(y) = 0$.
Let f_j be defined as in (3). By induction, there is a $m \geq 1$ and there are polynomials g_1, g_2 over R such that

$$f_s(x) = y \iff \exists w \in R^m : g_1(\bar{\tau}(x), \tau(y), w) = 0,$$

$$f_t(x) = y \iff \exists w \in R^m : g_2(\bar{\tau}(x), \tau(y), w) = 0.$$

Then we have that

$$f_j(x) = y \iff \exists v \in R^l : f_+(\tau(f_s(x)), \tau(f_t(x)), \tau(y), v) = 0$$

$$\iff \exists v \in R^l, w_1, w_2 \in R^m, z_1, z_2 \in \mathbb{Z} :$$

$$g_1(\bar{\tau}(x), \tau(z_1), w_1) = g_2(\bar{\tau}(x), \tau(z_2), w_2) = f_+(\tau(z_1), \tau(z_2), \tau(y), v) = 0$$

$$\iff \exists v \in R^l, w_1, w_2 \in R^m, u_1, u_2 \in \tau(\mathbb{Z}) :$$

$$g_1(\bar{\tau}(x), u_1, w_1) = g_2(\bar{\tau}(x), u_2, w_2) = f_+(u_1, u_2, \tau(y), v) = 0.$$

Since $\tau(\mathbb{Z})$ is diophantine over R, the assertion follows for f_j with Lemma 2.1.6. If f_j is defined as in (4), the construction of g can be done in a similar way using $f_\times$ instead of f_+.
All in all, we have shown that our assertion is true for all f_j and in particular for f.
Now let $A = \{x \in \mathbb{Z}^n | \exists y \in \mathbb{Z}^m : f(x, y) = 0\}$ be an arbitrary diophantine set over $\mathbb{Z}$ with $f \in \mathbb{Z}[x_1, \dots, x_n, y_1, \dots, y_m]$. There is a $p \in \mathbb{N}$ and a polynomial

$$g \in R[u_1, \dots, u_{k(n+m)}, v_1, \dots, v_k, w_1, \dots, w_p]$$

which fulfills

$$f(x, y) = z \iff \exists w \in R^p : g(\bar{\tau}(x), \bar{\tau}(y), \tau(z), w) = 0 \ \forall x \in \mathbb{Z}^n, y \in \mathbb{Z}^m, z \in \mathbb{Z}.$$

Thus, we can conclude that

$$\bar{\tau}(A) = \{u \in R^{kn} | \exists x \in \mathbb{Z}^n, y \in \mathbb{Z}^m : \bar{\tau}(x) = u, f(x, y) = 0\}$$

$$= \{u \in R^{kn} | \exists x \in \mathbb{Z}^n, y \in \mathbb{Z}^m, w \in R^p : \bar{\tau}(x) = u, g(\bar{\tau}(x), \bar{\tau}(y), \tau(0), w) = 0\}$$

$$= \{u \in \bar{\tau}(\mathbb{Z}^n) | \exists v \in \bar{\tau}(\mathbb{Z}^m), w \in R^p : g(u, v, \tau(0), w) = 0\}.$$

Therefore, $\bar{\tau}(A)$ is diophantine over R.
It remains to show that τ is computable under any computable presentation of R. Let $J : R \to \mathbb{N}$ be a computable presentation of R. By Lemma 2.1.10 the set $\bar{J}(D_+)$ is listable. Let $s : \mathbb{N} \to \mathbb{N}^{3k}$ be a computable function with $s(\mathbb{N}) = \bar{J}(D_+)$. We want to define a computable function $g : \mathbb{N} \to \mathbb{N}^k$ with $g \circ J_{\mathbb{Z}} = \bar{J} \circ \tau$. We set $g(1) := \bar{J}(\tau(0))$, $g(3) := \bar{J}(\tau(1))$ and $g(6) := \bar{J}(\tau(-1))$. Now let $m \geq 1$ and

assume that $g(3^{m-1})$ has already been defined. We define

$$n := \min\{l \in \mathbb{N} | \exists u \in \mathbb{N}^k : s(l) = (g(3), g(3^{m-1}), u)\}$$

and set $g(3^m) := (\pi_{2k+1}(s(n)), \dots, \pi_{3k}(s(n)))$. Similarly, if $g(2 \cdot 3^{m-1})$ is already defined, we define

$$n' := \min\{l \in \mathbb{N} | \exists u \in \mathbb{N}^k : s(l) = (g(3), g(2 \cdot 3^{m-1}), u)\}$$

and set $g(2 \cdot 3^m) := (\pi_{2k+1}(s(n')), \dots, \pi_{3k}(s(n')))$. If $t \in \mathbb{N}$ is not of the form 1, $2 \cdot 3^m$ or 3^m for some $m \geq 1$, we set $g(t) := 0$. Then g is a computable function and it follows with induction that $g(J_{\mathbb{Z}}(n)) = \bar{J}(\tau(n))$ for all $n \in \mathbb{Z}$. □

Remark 2.1.12. A perhaps more intuitive version of Definition 2.1.1 would be to call H10 decidable over R under J if there is a computable function $T : \bigcup_{n \geq 1} \mathbb{N}^n \to \{0, 1\}$ such that $T(t) = 1$ if and only if there is a $k \geq 1$ and a $f \in R[x_1, \dots, x_k]$ such that $C_{R,J}(f) = t$ and there is a $x \in R^k$ with $f(x) = 0$. This obviously results in a weaker definition of H10-decidability and a stronger definition of H10-undecidability. When using this definition, Theorem 2.1.5 can be proved in the same way if statement (2) is true, but it is not clear how to prove it for statement (1). Therefore, we also do not have Theorem 2.1.9. It should be mentioned though that since we use diophantine models of $\mathbb{Z}$ in chapter 3 and chapter 4, we could also use this definition and gain slightly stronger results.

2.2 H10 over $\mathbb{Q}$ and Mazur's Conjecture

Probably the most prominent unsolved problem in connection with H10 is the question if H10 is decidable over $\mathbb{Q}$. Before we start discussing this famous problem, we will state a computable presentation of $\mathbb{Q}$.

Theorem 2.2.1 (A presentation of $\mathbb{Q}$)**.** *Let $J_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{N}$ be defined as*

$$J_{\mathbb{Q}}\left(\frac{x}{y}\right) := J_{\mathbb{Z}}(x) \cdot 5^{y-1}$$

for $x \in \mathbb{Z} \setminus \{0\}$ and $y \in \mathbb{N} \setminus \{0\}$ with $(x, y) = 1$. Set $J_{\mathbb{Q}}(0) := 1$.
Then $J_{\mathbb{Q}}$ is a computable presentation of $\mathbb{Q}$ (as a field) which extends $J_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{N}$. In particular, $J_{\mathbb{Q}}(\mathbb{Z})$ is computable.

Proof: The function $J_{\mathbb{Q}}$ is injective due to the unique prime factorization for integers.
The set $J_{\mathbb{Q}}(\mathbb{Q}) = \{3^m 5^n | m, n \in \mathbb{N}\} \cup \{2 \cdot 3^m 5^n | m, n \in \mathbb{N}, m \geq 1\}$ can be written as

$$J_{\mathbb{Q}}(\mathbb{Q}) = \{1\} \cup \{n \in \mathbb{N} | \rho(1, n) = 0, 3 \leq \mu(n) \leq 5\} \cup \{n \in \mathbb{N} | \rho(1, n) = 1, \rho(2, n) \geq 1, 3 \leq \mu(n) \leq 5\}$$

which is a computable set by Lemma 1.2.6.
To show that addition is computable, we begin with defining functions to express the numerator and the denominator of a rational number under $J_{\mathbb{Q}}$. Let $N, D : \mathbb{N} \to \mathbb{N}$ be defined as $N(m) := 2^{\rho(1,m)} 3^{\rho(2,m)}$, $D(m) := 3^{\rho(3,m)+1}$. These functions are computable by Lemma 1.2.4 and 1.2.6. Recalling the definition of $J_{\mathbb{Z}}$, we obviously have $N(m), D(m) \in J_{\mathbb{Z}}(\mathbb{Z})$ for all $m \in J_{\mathbb{Q}}(\mathbb{Q})$.

Now if $k = 2^l 3^m 5^n \in J_{\mathbb{Q}}(\mathbb{Q})$, we have that

$$J_{\mathbb{Q}}\left(\frac{J_{\mathbb{Z}}^{-1}(N(k))}{J_{\mathbb{Z}}^{-1}(D(k))}\right) = J_{\mathbb{Q}}\left(\frac{J_{\mathbb{Z}}^{-1}(2^l 3^m))}{J_{\mathbb{Z}}^{-1}(3^{n+1}))}\right) = J_{\mathbb{Q}}\left(\frac{(-1)^l m}{n+1}\right) = 2^l 3^m 5^n = k.$$

Now recall the computable functions $J_{\mathbb{Z},+}$ and $J_{\mathbb{Z},\times}$ from the proof of Theorem 1.3.6. We define the addition of numerators and denominators separately. Let $N_+, D_+ : \mathbb{N}^2 \to \mathbb{N}$ be defined as $N_+(m,n) := J_{\mathbb{Z},+}(J_{\mathbb{Z},\times}(N(m), D(n)), J_{\mathbb{Z},\times}(N(n), D(m)))$ and $D_+(m,n) := J_{\mathbb{Z},\times}(D(m), D(n))$. These functions are computable since they are compositions of computable functions.
Now let $x = \frac{m_1}{n_1}, y = \frac{m_2}{n_2}, z = \frac{m_3}{n_3} \in \mathbb{Q}$ such that $x+y = z$ is fulfilled, $m_i, n_i \in \mathbb{Z}$ with $n_i > 0$ and either $(m_i = 0 \wedge n_i = 1)$ or $(m_i, n_i) = 1$ for $i \in \{1,2,3\}$. Then we have that $(m_1 n_2 + m_2 n_1) n_3 = (n_1 n_2) m_3$ and therefore

$$J_{\mathbb{Z},\times}(N_+(J_{\mathbb{Q}}(x), J_{\mathbb{Q}}(y)), D(J_{\mathbb{Q}}(z))) = J_{\mathbb{Z},\times}(D_+(J_{\mathbb{Q}}(x), J_{\mathbb{Q}}(y)), N(J_{\mathbb{Q}}(z))).$$

Thus, for every $(m,n) \in J_{\mathbb{Q}}(\mathbb{Q})^2$ the set

$$A_{m,n} := \{k \in J_{\mathbb{Q}}(\mathbb{Q}) | J_{\mathbb{Z},\times}(N_+(m,n), D(k)) = J_{\mathbb{Z},\times}(D_+(m,n), N(k))\}$$

is non-empty. Notice that the set is also computable. Thus, the relation $R_+ : \mathbb{N}^3 \to \{0,1\}$, $R_+(m,n,k) = 1 \iff (m,n) \notin J_{\mathbb{Q}}(\mathbb{Q})^2 \vee k \in A_{m,n}$ is computable and for every $(m,n) \in \mathbb{N}^2$ there is a $k \in \mathbb{N}$ such that $R(m,n,k) = 1$. Now we can define $J_{\mathbb{Q},+} : \mathbb{N}^2 \to \mathbb{N}$ as $J_{\mathbb{Q},+}(m,n) := \mu_k(R_+(m,n,k))$ which is computable by Definition 1.2.2. Then $J_{\mathbb{Q},+}(J_{\mathbb{Q}}(x), J_{\mathbb{Q}}(y)) = J_{\mathbb{Q}}(x+y)$ for all $x, y \in \mathbb{Q}$ due to the calculations above.
Recall the computable function g from the proof of Theorem 1.3.6 with the property that $J_{\mathbb{Z}}(-x) = (g \circ J_{\mathbb{Z}})(x)$ for all $x \in \mathbb{Z}$. Define a function $g_{\mathbb{Q}} : \mathbb{N} \to \mathbb{N}$,

$$g_{\mathbb{Q}}(m) := 2^{\rho(1, g(N(m)))} 3^{\rho(2,m)} 5^{\rho(3,m)}.$$

Obviously, $g_{\mathbb{Q}}$ is a computable function and $J_{\mathbb{Q}}(-x) = (g_{\mathbb{Q}} \circ J_{\mathbb{Q}})(x)$ for all $x \in \mathbb{Q}$. We define $J_{\mathbb{Q},-} : \mathbb{N}^2 \to \mathbb{N}$ as $J_{\mathbb{Q},-}(m,n) := J_{\mathbb{Q},+}(m, g_{\mathbb{Q}}(n))$ which is a computable function and has the property $J_{\mathbb{Q},-}(J_{\mathbb{Q}}(x), J_{\mathbb{Q}}(y)) = J_{\mathbb{Q}}(x-y)$ for all $x, y \in \mathbb{Q}$.
Considering multiplication, we define functions $N_\times, D_\times : \mathbb{N}^2 \to \mathbb{N}$ as $N_\times(m,n) := J_{\mathbb{Z},\times}(N(m), N(n))$ and $D_\times(m,n) := J_{\mathbb{Z},\times}(D(m), D(n))$. These functions are computable. Again, let $x = \frac{m_1}{n_1}$, $y = \frac{m_2}{n_2}, z = \frac{m_3}{n_3} \in \mathbb{Q}$ such that $xy = z$ is fulfilled, $m_i, n_i \in \mathbb{Z}$ with $n_i > 0$ and either $(m_i = 0 \wedge n_i = 1)$ or $(m_i, n_i) = 1$ for $i \in \{1,2,3\}$. Then $(m_1 m_2) n_3 = (n_1 n_2) m_3$ and thus the set

$$B_{m,n} := \{k \in J_{\mathbb{Q}}(\mathbb{Q}) | J_{\mathbb{Z},\times}(N_\times(m,n), D(k)) = J_{\mathbb{Z},\times}(D_\times(m,n), N(k))\}$$

is computable and non-empty for all $(m,n) \in J_{\mathbb{Q}}(\mathbb{Q})$. Define the relation $R_\times : \mathbb{N}^3 \to \{0,1\}$,

$$R_\times(m,n,k) = 1 \iff (m,n) \notin J_{\mathbb{Q}}(\mathbb{Q})^2 \vee k \in B_{m,n}$$

and define $J_{\mathbb{Q},\times} : \mathbb{N}^2 \to \mathbb{N}$, $J_{\mathbb{Q},\times}(m,n) := \mu_k(R_\times(m,n,k))$. This function is computable and fulfills $J_{\mathbb{Q},\times}(J_{\mathbb{Q}}(x), J_{\mathbb{Q}}(y)) = J_{\mathbb{Q}}(xy)$.

Lastly, we define the function $h : \mathbb{N} \to \mathbb{N}$, $h(m) := 2^{\rho(1,m)}3^{\rho(3,m)+1}5^{|\rho(2,m)-1|}$. This function is computable and for $x = (-1)^k \frac{m}{n} \in \mathbb{Q}^*$ with $k \in \{0,1\}$, $m, n > 0$ and $(m,n) = 1$ it fulfills:

$$h(J_{\mathbb{Q}}(x)) = h(2^k 3^m 5^{n-1}) = 2^k 3^n 5^{|m-1|} = 2^k 3^n 5^{m-1} = J_{\mathbb{Q}}\left((-1)^k \frac{n}{m}\right) = J_{\mathbb{Q}}\left(\frac{1}{x}\right)$$

So we can define $J_{\mathbb{Q},/} : \mathbb{N}^2 \to \mathbb{N}$ as $J_{\mathbb{Q},/}(m,n) := J_{\mathbb{Q},\times}(m, h(n))$. This is a computable function and fulfills $J_{\mathbb{Q},/}(J_{\mathbb{Q}}(x), J_{\mathbb{Q}}(y)) = J_{\mathbb{Q}}(\frac{x}{y})$ for all $x \in \mathbb{Q}$, $y \in \mathbb{Q}^*$.
For the second statement it suffices to observe that $J_{\mathbb{Q}}(x) = J_{\mathbb{Z}}(x)$ for all $x \in \mathbb{Z}$, and thus the set $J_{\mathbb{Q}}(\mathbb{Z}) = J_{\mathbb{Z}}(\mathbb{Z})$ is computable. □

We know from Theorem 1.3.7 that all computable presentations of $\mathbb{Q}$ are equivalent. Therefore, these presentations are extensions of $J_{\mathbb{Z}}$. One possible way to prove that H10 is undecidable over $\mathbb{Q}$ would be to show that $\mathbb{Z}$ has a diophantine definition over $\mathbb{Q}$ (since all other requirements of Theorem 2.1.9 are obviously met). Another strategy would be to find a diophantine model of $\mathbb{Z}$ in $\mathbb{Q}$.
However, in 1992 Barry Mazur made the following conjecture in [8] which implies both that there is no diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$ and that there is no tight diophantine model of $\mathbb{Z}$ in $\mathbb{Q}$ (the latter fact was first proved by Gunther Cornelissen and Karim Zahidi in [1]). See also chapter 12 of [15] for a discussion of Mazur's conjecture.

Conjecture 2.2.2 (Mazur)**.** *Let V be any variety over $\mathbb{Q}$. Then the Euclidean closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ has only finitely many connected components.*

Up until now, Mazur's conjecture has only been proved for 1-dimensional varieties (curves).
Before stating and proving the consequences of Mazur's conjecture, we will prove a lemma which will assure us that, if the conjecture is true, also the closures of diophantine sets over $\mathbb{Q}$ will only have finitely many connected components.

Lemma 2.2.3. *Let T_1, T_2 be topological spaces. Consider the space $T_1 \times T_2$ endowed with the product topology. Let $\pi_1 : T_1 \times T_2 \to T_1$ be the first projection. If the closure $\overline{S}$ of a set $S \subseteq T_1 \times T_2$ has only finitely many connected components, the set $\overline{\pi_1(S)}$ also has only finitely many connected components.*

Proof: Assume that $\overline{\pi_1(S)} = \bigcup_{i \in J} C_i$ with J an infinite index set and $C_i \subseteq T_1$ non-empty, closed and pairwise disjoint. Then $C_i \cap \pi_1(S) \neq \emptyset$ for infinitely many $i \in J$ (as $\pi_1(S) \subseteq \bigcup_{i \in I} C_i$ with $I \subseteq J$ finite would imply that $\overline{\pi_1(S)}$ is a subset of $\overline{\bigcup_{i \in I} C_i} = \bigcup_{i \in I} C_i$). Since $\pi_1^{-1}(\overline{\pi_1(S)})$ is a closed set containing S, we have that $\overline{S} \subseteq \pi_1^{-1}(\overline{\pi_1(S)})$. This implies that $\overline{S} = \bigcup_{i \in J}(\overline{S} \cap \pi_1^{-1}(C_i))$ where the elements of this union are closed and pairwise disjoint and infinitely many are non-empty. But this is a contradiction to our assumption that $\overline{S}$ has only finitely many connected components. □

Theorem 2.2.4 (Consequences of Mazur's conjecture)**.** *Assume that Conjecture 2.2.2 is true. Then the following two statements are true:*

(1) *There is no diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.*

(2) *$\mathbb{Q}$ has no tight diophantine model of $\mathbb{Z}$.*

Proof of (1): Assume that there is a defining polynomial $f \in \mathbb{Q}[x, y_1, \ldots, y_n]$ such that

$$\mathbb{Z} = \{x \in \mathbb{Q} | \exists y \in \mathbb{Q}^n : f(x, y) = 0\}.$$

Now consider the variety V over $\mathbb{Q}$ which is defined by f. By Mazur's conjecture, $\overline{V(\mathbb{Q})} \subseteq V(\mathbb{R})$ has only finitely many connected components. Consider the first projection $\pi_1 : \mathbb{R}^{n+1} \to \mathbb{R}$. It follows with Lemma 2.2.3 that $\overline{\pi_1(V(\mathbb{Q}))} \subseteq \mathbb{R}$ has only finitely many components. But now we have that $\pi_1(V(\mathbb{Q})) = \{x \in \mathbb{Q} | \exists y \in \mathbb{Q}^n : f(x, y) = 0\} = \mathbb{Z}$ and since $\overline{\mathbb{Z}} \subseteq \mathbb{R}$ is an infinite discrete set, this is a contradiction. □

Proof of (2): Assume that $\mathbb{Q}$ has a tight diophantine model of $\mathbb{Z}$. Then there is a computable map $\Phi : \mathbb{Z} \to \mathbb{Q}^n$ such that $\Phi(A) \subseteq \mathbb{Q}^n$ is a diophantine set for every diophantine set $A \subseteq \mathbb{Z}$. Therefore, $D := \Phi(\mathbb{Z}) \subseteq \mathbb{Q}^n$ is a diophantine set. Exactly in the same way as in the proof of (1), it follows that $\overline{D} \subseteq \mathbb{R}^n$ has only finitely many connected components. Since Φ is injective by Lemma 2.1.4, D is an infinite set and there is a connected component C of $\overline{D}$ such that $C \cap D$ is not just a point. There is a $i \in \{1, \ldots, n\}$ such that the projection $\pi_i(C) \subseteq \mathbb{R}$ contains an interval $[a, a + l]$ with $a, l \in \mathbb{Q}$. Now define a map $d : \mathbb{Z} \to \mathbb{Q}$, $d := \pi_i \circ \Phi$ and a set:

$$\tilde{Z} := \left\{ n \in \mathbb{Z} \middle| \exists j \geq 1 : a + \frac{l}{2j+1} \leq d(n) \leq a + \frac{l}{2j} \right\}.$$

The set $\tilde{Z} \subseteq \mathbb{Z}$ is listable since $d = \pi_i \circ \Phi$ is computable and for every pair $(n, j) \in \mathbb{Z} \times \mathbb{Z}_{>0}$ we can compute whether $a + \frac{l}{2j+1} \leq d(n) \leq a + \frac{l}{2j}$ is fulfilled. With Theorem 1.4.3 we can conclude that $\tilde{Z}$ is a diophantine set. Therefore, $\tilde{D} := \Phi(\tilde{Z})$ is diophantine over $\mathbb{Q}$. It follows again from Mazur's Conjecture that $\overline{\tilde{D}}$ has only finitely many connected components. Since $[a, a + l] \cap \pi_i(D)$ is dense in $[a, a + l]$, it follows from the definition of $\tilde{Z}$ that $\pi_i(\tilde{D})$ is dense in the set

$$\{x \in \mathbb{R} | \exists j \geq 1 : a + \frac{l}{2j+1} \leq x \leq a + \frac{l}{2j}\}.$$

But this implies that $\overline{\tilde{D}} \subseteq \bigcup_{j \geq 1} C_j$ and $\tilde{D} \cap C_j \neq \emptyset$ for all $j \geq 1$ where

$$C_j := \left\{ x = (x_1, \ldots, x_n) \in \mathbb{R}^n \middle| a + \frac{l}{2j+1} \leq x_i \leq a + \frac{l}{2j} \right\}.$$

But this clearly implies that $\overline{\tilde{D}}$ has infinitely many connected components and this poses a contradiction. □

2.3 H10 over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$

One way of approaching the unresolved problems of H10 over $\mathbb{Q}$ and Mazur's conjecture is to investigate the analogous problems for rings R with $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$. In fact, we will show in chapter 3 that we can find subrings of $\mathbb{Q}$, which are very large in a certain sense, for which both Mazur's conjecture is false and H10 is undecidable.
As a preparation, we will investigate the computability and diophantine properties of subrings of $\mathbb{Q}$

in this section. We start with a characterization of these rings.

Definition 2.3.1 (Rings of $\mathcal{W}$-Integers)**.** Let $\mathcal{W} \subseteq \mathcal{P}$ be a set of prime numbers. Then we define the ring of $\mathcal{W}$-Integers as

$$\mathcal{O}_{\mathbb{Q},\mathcal{W}} := \{x \in \mathbb{Q} | \forall p \notin \mathcal{W} : \mathrm{ord}_p(x) \geq 0\}.$$

Theorem 2.3.2. *Let R be a ring with $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$. Then R is of the form $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ for some set $\mathcal{W} \subseteq \mathcal{P}$.*

Proof: Let $\mathcal{W} := \{p \in \mathcal{P} | \frac{1}{p} \in R\}$. It is obvious that $\mathcal{O}_{\mathbb{Q},\mathcal{W}} \subseteq R$. Now suppose that there is a $x \in R$ with $\mathrm{ord}_p(x) < 0$ for a $p \notin \mathcal{W}$. Then $x = \frac{y}{zp}$ with $y \in \mathbb{Z}$, $z \geq 1$ and $(y, p) = 1$. It follows that $\frac{y}{p} \in R$. Since $(y, p) = 1$, there are $m, n \in \mathbb{Z}$ such that $ym + pn = 1$. It follows that

$$\frac{1}{p} = \frac{ym + pn}{p} = m\frac{y}{p} + n \in R.$$

But this would imply that $p \in \mathcal{W}$ which is a contradiction. Thus, we have that $R \subseteq \mathcal{O}_{\mathbb{Q},\mathcal{W}}$ which proves our assertion. □

We can also give a simple classification of the subrings of $\mathbb{Q}$ which are computable.

Theorem 2.3.3 (Computability of $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$)**.** *Let $\mathcal{W} \subseteq \mathcal{P}$ be a set of prime numbers. The ring $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ is computable under $J_{\mathbb{Q}}$ (and thus, under any computable presentation of $\mathbb{Q}$ by Theorem 1.3.7) if and only if $\mathcal{W} \subseteq \mathbb{N}$ is computable.*

Proof: We begin with showing that the set of primes $\mathcal{W} \subseteq \mathcal{P}$ is computable if and only if the set $\langle \mathcal{W} \rangle := \{x \in \mathbb{N}_{>0} | \forall p \notin \mathcal{W} : \mathrm{ord}_p(x) = 0\} \subseteq \mathbb{N}$ is computable.
Recall the definitions of the computable functions ρ, ϕ and g from Lemma 1.2.6. Then we have for every set of prime numbers $\mathcal{W} \subseteq \mathcal{P}$ that

$$\chi_{\langle \mathcal{W} \rangle}(m) = \prod_{i=1}^{g(\mu(m))} \left(\chi_{\mathcal{W}}(\phi(m)) \,\mathrm{sgn}(\rho(i, m)) + \overline{\mathrm{sgn}}(\rho(i, m)) \right)$$

(notice that this function is computable when $\chi_{\mathcal{W}}$ is computable by Lemma 1.2.5) and

$$\chi_{\mathcal{W}}(m) = \chi_{\mathcal{P}}(m)\chi_{\langle \mathcal{W} \rangle}(m).$$

Thus, the assertion is proved. But now we also have that

$$\chi_{J_{\mathbb{Q}}(\mathcal{O}_{\mathbb{Q},\mathcal{W}})}(m) = \chi_{J_{\mathbb{Q}}(\mathbb{Q})}(m)\chi_{\langle \mathcal{W} \rangle}(\rho(3, m) + 1)$$

and

$$\chi_{\langle \mathcal{W} \rangle}(m) = \chi_{J_{\mathbb{Q}}(\mathcal{O}_{\mathbb{Q},\mathcal{W}})}(3 \cdot 5^{m-1}).$$

This proves our initial assertion. □

All rings $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ have an important diophantine property which will be described in the following definition:

Definition 2.3.4 (Dioph-regularity)**.** Let R be a ring. R is called dioph-regular if the set $R \setminus \{0\}$ is a diophantine subset of R.

Theorem 2.3.5 ($\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ is dioph-regular)**.** *Let $\mathcal{W} \subseteq \mathcal{P}$ be any set of prime numbers. Then the ring $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ is dioph-regular.*

Proof: We will only give a proof for the case in which $\#(\mathcal{P} \setminus \mathcal{W}) \geq 2$ (a complete proof can be found in [15], p. 24-25). So let $p, q \in \mathcal{P} \setminus \mathcal{W}$ with $p \neq q$. We want to show that

$$\mathcal{O}_{\mathbb{Q},\mathcal{W}} \setminus \{0\} = \{x \in \mathcal{O}_{\mathbb{Q},\mathcal{W}} | \exists u, v, w \in \mathcal{O}_{\mathbb{Q},\mathcal{W}} : xu - (pv-1)(qw-1) = 0\}.$$

Suppose that $x = 0$ and there are $u, v, w \in \mathcal{O}_{\mathbb{Q},\mathcal{W}}$ with $0 = xu = (pv-1)(qw-1)$. Then either p or q is invertible in $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ which is not possible since $p, q \notin \mathcal{W}$.
Now suppose that $x \in \mathcal{O}_{\mathbb{Q},\mathcal{W}} \setminus \{0\}$. Let $x = \frac{a_1 a_2}{b}$ with $a_1, a_2 \in \mathbb{Z}$, $b \geq 1$ and $(a_1, p) = (a_2, q) = 1$. Then it follows from the Chinese remainder theorem that there are $v, w \in \mathbb{Z}$ with $pv \equiv 1 \pmod{a_1}$ and $qw \equiv 1 \pmod{a_2}$. Thus, $(pv-1)(qw-1) \equiv 0 \pmod{a_1 a_2}$ and there is a $m \in \mathbb{Z}$ with

$$(pv-1)(qw-1) = ma_1a_2 = (mb)x.$$

□

An important property of dioph-regular rings is described in the following lemma:

Lemma 2.3.6. *Let R be a dioph-regular ring and K its quotient field. Assume that K is not algebraically closed. If $D \subseteq K^n$ is diophantine over K, then $D \cap R^n$ is diophantine over R.*

Proof: We can find a polynomial $f(x, y) \in R[x_1, \ldots, x_n, y_1, \ldots, y_m]$ such that

$$D = \{x \in K^n | \exists y \in K^m : f(x, y) = 0\}.$$

Then we have that

$$D \cap R^n = \{x \in R^n | \exists y \in K^m : f(x, y) = 0\}$$

$$= \{x \in R^n | \exists y, z \in R^m : z_1 \neq 0, \ldots, z_m \neq 0, f(x, y_1/z_1, \ldots, y_m/z_m) = 0\}.$$

Now we define a new polynomial $F \in R[x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, \ldots, z_m]$,

$$F(x, y, z) := (z_1 \cdots z_n)^{\deg(f)} f(x, y_1/z_1, \ldots, y_m/z_m)$$

and conclude that

$$D \cap R^n = \{x \in R^n | \exists y, z \in R^m : z_1 \neq 0, \ldots, z_m \neq 0, F(x, y, z) = 0\}.$$

This gives us a diophantine definition of $D \cap R^n$ over R with Lemma 2.1.6 since the ring R is dioph-regular. □

If $\mathcal{S} \subseteq \mathcal{P}$ is a finite set of prime numbers, the rings $\mathcal{O}_{\mathbb{Q},\mathcal{S}}$ and $\mathcal{O}_{\mathbb{Q},\mathcal{P}\setminus\mathcal{S}}$ are computable rings by Theorem 2.3.3. We have the following result for these rings (which is discussed in chapter 4 of [15]):

Theorem 2.3.7. *Let $\mathcal{S} \subseteq \mathcal{P}$ be a finite set of prime numbers. Then $\mathcal{O}_{\mathbb{Q},\mathcal{P}\setminus\mathcal{S}}$ has a diophantine definition over $\mathbb{Q}$.*

Corollary 2.3.8. *Let $\mathcal{S} \subseteq \mathcal{P}$ be a finite set of prime numbers. Then H10 is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{S}}$.*

Proof: By Theorem 2.3.7, $\mathcal{O}_{\mathbb{Q},\mathcal{P}\setminus\mathcal{S}}$ is diophantine in $\mathbb{Q}$. Since the ring $\mathcal{O}_{\mathbb{Q},\mathcal{S}}$ is dioph-regular by Theorem 2.3.5, Lemma 2.3.6 implies that $\mathcal{O}_{\mathbb{Q},\mathcal{P}\setminus\mathcal{S}} \cap \mathcal{O}_{\mathbb{Q},\mathcal{S}} = \mathbb{Z}$ is diophantine in $\mathcal{O}_{\mathbb{Q},\mathcal{S}}$. Now we can conclude with Theorem 2.1.9 that H10 is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{S}}$. □

To measure the size of a ring $\mathcal{O}_{\mathbb{Q},\mathcal{W}} \subseteq \mathbb{Q}$, we will use the *density* of the set $\mathcal{W} \subseteq \mathcal{P}$. There are several related definitions for the density of a set of prime numbers. We will use the notion of *natural density*.

Definition 2.3.9 (Natural density)**.** For a set of primes $\mathcal{W} \subseteq \mathcal{P}$ we define its natural density as

$$\delta_{nat}(\mathcal{W}) := \lim_{n\to\infty} \frac{\#\{p \in \mathcal{W} | p \leq n\}}{\pi_{\mathbb{Q}}(n)}$$

and its upper natural density as

$$\delta^{up}_{nat}(\mathcal{W}) := \limsup_{n\to\infty} \frac{\#\{p \in \mathcal{W} | p \leq n\}}{\pi_{\mathbb{Q}}(n)}.$$

Examples 2.3.10.

- $\delta_{nat}(\mathcal{P}) = 1$.
- $\delta_{nat}(\mathcal{W}) = 0$ for every finite set $\mathcal{W}$, but there are also infinite sets of primes with natural densitiy zero.

3 Poonen's theorem

3.1 The theorem and its consequences

The theorem which we will discuss in this chapter was first proved by Bjorn Poonen in [10]. The proof which we will use is mainly orientated towards the theorem's proof in chapter 12 of [15]. Poonen's theorem constituted a big step towards solving H10 over $\mathbb{Q}$ since it proved H10 undecidable for the first time for a ring $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ with an infinite set of prime numbers $\mathcal{W}$. In fact, $\mathcal{W}$ can even be chosen in such a way that the natural density of $\mathcal{W}$ is equal to 1. What keeps us from proving that H10 is undecidable over $\mathbb{Q}$ along the way is the fact that $\mathcal{P} \setminus \mathcal{W}$ is still an infinite set. (If $\mathcal{P} \setminus \mathcal{W}$ would be finite, then $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ would have diophantine definition over $\mathbb{Q}$ by Theorem 2.3.7 and with Theorem 2.1.9 it would follow that H10 is undecidable over $\mathbb{Q}$.)

Theorem 3.1.1 (Poonen)**.** *There are computable, disjoint sets of prime numbers $T_1, T_2 \subseteq \mathcal{P}$ with $\delta_{nat}(T_1) = \delta_{nat}(T_2) = 0$ such that for every set of primes $\mathcal{W} \subseteq \mathcal{P}$, fulfilling $T_1 \subseteq \mathcal{W} \subseteq \mathcal{P} \setminus T_2$, the ring $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ has a diophantine model of $\mathbb{Z}$.*

Corollary 3.1.2. *There is a computable set of primes $\mathcal{W} \subseteq \mathcal{P}$ with $\delta_{nat}(\mathcal{W}) = 1$ such that H10 is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$.*

Proof: Choose $\mathcal{W} := \mathcal{P} \setminus T_2$. Then we have that $\delta_{nat}(\mathcal{W}) = \delta_{nat}(\mathcal{P}) - \delta_{nat}(T_2) = 1$. The set $\mathcal{W}$ is computable since $\mathcal{P}$ and T_2 are computable. Therefore, $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ is a computable ring by Theorem 2.3.3. Since T_1, T_2 are disjoint, also $T_1 \subseteq \mathcal{W}$ is fulfilled. Then by Theorem 3.1.1, $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ has a diophantine model of $\mathbb{Z}$. With Theorem 2.1.5 it follows that H10 is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$. □

For the construction of the sets $T_1, T_2 \subseteq \mathcal{P}$ we will use an elliptic curve with special properties (more specifically, T_1 and T_2 will be constructed from the prime divisors of certain rational points on the curve). Therefore, the entire next section will be devoted to elliptic curves. We will prove several facts which will be crucial for our proof of Theorem 3.1.1 and also state a number of results for which we will not give a proof (especially those results for which a proof can be found in [16]).

3.2 Properties of elliptic curves

Since it would go beyond our scope to give an adequate introduction to the theory of elliptic curves, we refer the reader to [16] as our main reference. There one can find an introduction as well as many results which we will need on our way to prove Theorem 3.1.1. We start with the observation that there is an elliptic curve over $\mathbb{Q}$ with some convenient properties.

Theorem 3.2.1. *There is an elliptic curve E over $\mathbb{Q}$ with the following properties:*

- $E(\mathbb{Q}) =< P >\cong \mathbb{Z}$.
- *E has a Weierstrass equation of the form $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$.*
- $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ *as topological groups.*
- *E does not have complex multiplication (thus,* $\mathrm{End}(E) \cong \mathbb{Z}$*).*

Proof: Let E be the curve defined by the equation $y^2 = x^3 + x + 1$. This curve has conductor 496 and appears as A1 in Cremona's tables in [2]. $E(\mathbb{Q}) \cong \mathbb{Z}$ can be read off [2]. Since the determinant of E is $\Delta = -2^4 31$, $E(\mathbb{R})$ is isomorphic to $\mathbb{R}/\mathbb{Z}$ by Corollary 2.3.1, Chapter V of [18]. Finally, the j-invariant of E is $j = 2^8 3^3 31^{-1}$. Suppose that E does have complex multiplication. Then the j-invariant of E would have to be an integer by Theorem 6.1, Chapter II of [18]. This leads to a contradiction. □

For the rest of this chapter (except where explicitly mentioned otherwise) we will fix an elliptic curve E over $\mathbb{Q}$ together with a Weierstrass equation which fulfill the properties of Theorem 3.2.1. We also fix a point P on $E(\mathbb{Q})$ which generates the Abelian group $E(\mathbb{Q})$. We will denote the neutral element of E with $\mathcal{O}$.
Our first observation concerning E is that, since the affine Weierstrass equation is monic in x and y, every affine point $Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ is of the form $Q = (\frac{a}{b^2}, \frac{c}{b^3})$ with $a, b, c \in \mathbb{Z}$ where $b \geq 1$ and $(ac, b) = 1$. We will now introduce some specialized notation for our handling of E and especially the prime divisors of the rational points $n \cdot P$.

Notation:

- For $n \geq 1$ and K a field extension of $\mathbb{Q}$ let $E(K)[n] := \{Q \in E(K) | n \cdot Q = \mathcal{O}\}$.
- For $n \geq 1$, $p \in \mathcal{P}$ and $K = \mathbb{Q}$ or $K = \mathbb{Q}_p$ let

$$E_n(K) := \{Q = (x, y) \in E(K) \setminus \{\mathcal{O}\} | \operatorname{ord}_p(x) \leq -2n, \operatorname{ord}_p(y) \leq -3n\} \cup \{\mathcal{O}\}.$$

- For a point $Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ with affine coordinates $Q = (a, b)$ set $x(Q) := a$ and $y(Q) := b$. Further, let $Q^n := (a^n, b^n)$ for $n \geq 1$.
- Let $x_n := x(n \cdot P)$, $y_n := y(n \cdot P)$ for $n \in \mathbb{Z} \setminus \{0\}$.
- If K is a finite extension of $\mathbb{Q}$, let $S_0(K)$ be the set of primes $\mathfrak{p}$ of K that are either ramified over $\mathbb{Q}$ or divide the discriminant of the chosen Weierstrass equation of E. Notice that $2 \in S_0(\mathbb{Q})$ since the discriminant of a Weierstrass equation of the form $y^2 = x^3 + Ax + B$ is $\Delta = -16(4A^3 + 27B^2)$. If $\mathfrak{p} \notin S_0(K)$, let $\pi_\mathfrak{p} : E(K_\mathfrak{p}) \to E(\mathbb{F}_\mathfrak{p})$ denote the reduction of $E(K_\mathfrak{p})$ modulo $\mathfrak{p}$. Notice that $E(K_\mathfrak{p})$ is non-singular by Proposition 5.1, Chapter VIII of [16], p. 180. Let $\tilde{\mathcal{O}}$ denote the neutral element of $E(\mathbb{F}_\mathfrak{p})$.
- For $n \in \mathbb{Z} \setminus \{0\}$ let

$$S_n(P) := \{p \in \mathcal{P} | p \notin S_0(\mathbb{Q}), \operatorname{ord}_p(x_n) < 0\} = \{p \in \mathcal{P} | p \notin S_0(\mathbb{Q}), \operatorname{ord}_p(y_n) < 0\}.$$

- For $n \in \mathbb{Z} \setminus \{0\}$ let $d_n(P) := \prod_{l \in S_n(P)} l^{-\operatorname{ord}_l(x_n)} \in \mathbb{N}$.
- For $l \in \mathcal{P}$ set $a_l(P) := \min\{n \in \mathbb{N} | S_{l^n}(P) \setminus S_1(P) \neq \emptyset\}$. We will show that $a_l(P)$ is always well-defined in Corollary 3.2.3.
- Let $\mathcal{L}(P) := \{l \in \mathcal{P} | a_l(P) > 1\}$.
- For $l \in \mathcal{P}$ let $p_l(P) := \max(S_{l^{a_l(P)}}(P) \setminus S_1(P))$.
- For $l, p \in \mathcal{P}$ let $p_{l,p}(P) := \max(S_{lp}(P) \setminus (S_l(P) \cup S_p(P)))$ if the difference is not empty.
- For $l \in \mathcal{P}$ let
$$\mu_l(P) := \sup_{n \geq 2} \frac{\#\{p \in S_l(P) \setminus S_1(P) | p \leq n\}}{\pi_{\mathbb{Q}}(n)}.$$

To show that $a_l(P)$ is always well-defined we will employ a theorem of Carl Ludwig Siegel (Corollary 3.2.1, Chapter IX in [16], p. 248):

Theorem 3.2.2 (Siegel)**.** *Let E be an elliptic curve over $\mathbb{Q}$ in Weierstrass form and $\mathcal{W} \subseteq \mathcal{P}$ a finite set of prime numbers. Then the set*

$$\{Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\} | x(Q) \in \mathcal{O}_{\mathbb{Q},\mathcal{W}}\}$$

is finite.

Corollary 3.2.3. (1) *For every $l \in \mathcal{P}$ the value $a_l(P)$ is well-defined.*

(2) *There are only finitely many l with $a_l(P) > 1$ (thus, $\mathcal{L}(P)$ is a finite set).*

Proof: Since $\mathcal{W} := S_0(\mathbb{Q}) \cup S_1(P)$ is a finite set, there are only finitely many $Q \in E(\mathbb{Q})$ with $x(Q) \in \mathcal{O}_{\mathbb{Q},\mathcal{W}}$ by Theorem 3.2.2. In particular, there are only finitely many $n \geq 1$ with $x_{l^n} \in \mathcal{O}_{\mathbb{Q},\mathcal{W}}$. Thus, there is a $n \geq 1$ and a prime number $p \notin S_0(\mathbb{Q}) \cup S_1(P)$ with $\operatorname{ord}_p(x_{l^n}) < 0$. It follows that $p \in S_{l^n}(P)$ and hence $S_{l^n}(P) \setminus S_1(P) \neq \emptyset$.
The same argument implies that there are only finitely many $l \in \mathcal{P}$ with $x_l \in \mathcal{O}_{\mathbb{Q},\mathcal{W}}$. Thus, there are only finitely many l with $S_l(P) \subseteq S_1(P)$ and $a_l(P) = 1$ for all others. This implies our second statement. □

Next we will introduce the *formal group* associated to E (see Chapter IV of [16] for an exhaustive exposition of this topic).

Construction of the formal group associated to E:
We start with a change of coordinates:

$$z = -\frac{x}{y}, \; w = -\frac{1}{y}.$$

Notice that $\mathcal{O}$ now has the affine coordinates $(z, w) = (0, 0)$. The given Weierstrass equation of E

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

becomes

$$w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3 =: f(z, w). \tag{3.2.1}$$

There is a (as shown in Proposition 1.1, Chapter IV in [16], p. 111-112) unique power series

$$w(z) = z^3(1 + A_1 z + A_2 z^2 + \ldots) \in \mathbb{Z}[\![z]\!] \tag{3.2.2}$$

fulfilling $w(z) = f(z, w(z))$. Thus, $w(z)$ can be interpreted as a *formal solution* to (3.2.1). If z_1, z_2 are two independent indeterminates, we can sum the two points $(z_1, w(z_1))$, $(z_2, w(z_2))$ using the addition law on the transformed curve E and we get a point $(z_3, w(z_3))$. This *formal addition* can be expressed through a power series $F(z_1, z_2) = z_1 + z_2 + (\text{terms of degree} \geq 2) \in \mathbb{Z}[\![z_1, z_2]\!]$. Thus, we have that

$$(z_1, w(z_1)) +_E (z_2, w(z_2)) = (F(z_1, z_2), w(F(z_1, z_2))).$$

Notice that this is an identity of formal power series, not actually involving any points on the curve E. Inversion on E can also be expressed through a power series $i(z) = -z + (\text{terms of degree} \geq 2) \in \mathbb{Z}[\![z]\!]$. Thus,

$$-_E(z, w(z)) = (i(z), w(i(z))).$$

The power series $F(z_1, z_2)$ is called the *formal group associated to* E and is denoted as $\hat{E}$ (see [16], p. 115 for the definition of a formal group). From the corresponding properties of E we deduce that $F(z_1, z_2)$ has the following properties:

(1) $F(z_1, F(z_2, z_3)) = F(F(z_1, z_2), z_3)$,

(2) $F(0, z) = z$ and $F(z, i(z)) = 0$,

(3) $F(z_1, z_2) = F(z_2, z_1)$.

Reverting our change of coordinates we can define two Laurent series:

$$x(z) = \frac{z}{w(z)}, \; y(z) = -\frac{1}{w(z)}. \tag{3.2.3}$$

Then $(x(z), y(z))$ is a formal solution to our original Weierstrass equation of E. If we choose $z \in \mathcal{M}_p$ for any $p \in \mathcal{P}$, then $(x(z), y(z))$ converges to a point $(x, y) \in E(\mathbb{Q}_p)$.

Definition 3.2.4. Let $p \in \mathcal{P}$. We define $\hat{E}(\mathcal{M}_p)$ to be the set $\mathcal{M}_p$ with the group operations

$$z_1 \oplus_F z_2 := F(z_1, z_2) \text{ (addition) for } z_1, z_2 \in \mathcal{M}_p,$$

$$\ominus_F z := i(z) \text{ (inverse) for } z \in \mathcal{M}_p.$$

$\hat{E}(\mathcal{M}_p)$ is a group since

$$\mathrm{ord}_p(F(z_1, z_2)) = \mathrm{ord}_p(z_1 + z_2 + \ldots) \geq \min\{\mathrm{ord}_p(z_1), \mathrm{ord}_p(z_2)\} > 0,$$

$$\mathrm{ord}_p(i(z)) = \mathrm{ord}_p(-z + \ldots) \geq \mathrm{ord}_p(z) > 0.$$

In the same way we define the group $\hat{E}(\mathcal{M}_p^n)$ for all $n \geq 1$.

Then we have that

$$(x(z_1), y(z_1)) +_E (x(z_2), y(z_2)) = (x(z_1 \oplus_F z_2), y(z_1 \oplus_F z_2)) \; \forall z_1, z_2 \in \mathcal{M}_p.$$

In other words, we have a group homomorphism $\Phi : \hat{E}(\mathcal{M}_p) \to E(\mathbb{Q}_p)$ with $\Phi(z) := (x(z), y(z))$ for $z \neq 0$ and $\Phi(0) := \mathcal{O}$. In fact, even more is true:

Lemma 3.2.5. *The map $\Phi : \hat{E}(\mathcal{M}_p) \to E_1(\mathbb{Q}_p)$ is a group isomorphism.*

This is Proposition 2.2, Chapter VII in [16], p. 174-175.
Utilizing this lemma, we obtain our first important result concerning $d_n(P)$, the part of the denominator of x_n which is relatively prime to the prime numbers in $S_0(\mathbb{Q})$.

Lemma 3.2.6. *For every $p \in \mathcal{P}$ and $n \geq 1$,*

$$\{m \in \mathbb{Z} \setminus \{0\} : \mathrm{ord}_p(x_m) \leq -n\} \cup \{0\}$$

is a subgroup of $(\mathbb{Z}, +)$.

Proof: With (3.2.2) and (3.2.3) it follows that

$$\mathrm{ord}_p(z) = n \iff \mathrm{ord}_p(x(z)) = -2n \wedge \mathrm{ord}_p(y(z)) = -3n.$$

Thus, the map $\Phi : \hat{E}(\mathcal{M}_p^n) \to E_n(\mathbb{Q}_p) \subseteq E_1(\mathbb{Q}_p)$ is bijective for all $n \geq 1$. With Lemma 3.2.5 it follows that $E_n(\mathbb{Q}_p)$ is a group for all $n \geq 1$. Now we have that

$$\{m \in \mathbb{Z} \setminus \{0\} : \mathrm{ord}_p(x_m) \leq -2n\} \cup \{0\} = \{m \in \mathbb{Z} | m \cdot P \in E_n(\mathbb{Q})\} \cong E_n(\mathbb{Q}) = E_n(\mathbb{Q}_p) \cap E(\mathbb{Q})$$

which proves our assertion since $x_n = A_n/B_n^2$ with $A_n, B_n \in \mathbb{Z}$ such that $(A_n, B_n) = 1$, $B_n \geq 1$ for all $n \neq 0$. □

Corollary 3.2.7. *Let $p \in \mathcal{P}$. Then $G_p := \{m \in \mathbb{Z} \setminus \{0\} : p \mid d_m(P)\} \cup \{0\}$ is a subgroup of $(\mathbb{Z}, +)$.*

Proof: If $p \in S_0(\mathbb{Q})$, then $\mathrm{ord}_p(d_m(P)) = 0$ for all $m \in \mathbb{Z} \setminus \{0\}$ and consequently $G_p = \{0\}$.
Now suppose that $p \notin S_0(\mathbb{Q})$. Then we have that

$$G_p = \{m \in \mathbb{Z} \setminus \{0\} : p \mid d_m(P)\} \cup \{0\} = \{m \in \mathbb{Z} \setminus \{0\} : \mathrm{ord}_p(x_m) \leq -1\} \cup \{0\}.$$

This is a subgroup of $(\mathbb{Z}, +)$ by Lemma 3.2.6. □

We now can state and proof the first crucial theorem which will be used in the proof of Poonen's theorem.

Theorem 3.2.8. *$S_m(P) \cap S_n(P) = S_{(m,n)}(P)$ for all $m, n \in \mathbb{Z} \setminus \{0\}$.*

Proof: Notice that for every $k \in \mathbb{Z} \setminus \{0\}$ and $p \in \mathcal{P} \setminus S_0(\mathbb{Q})$ we have that

$$p \in S_k(P) \iff p \mid d_k(P) \iff k \in G_p = \{l \in \mathbb{Z} \setminus \{0\} : p \mid d_l(P)\} \cup \{0\}.$$

Since G_p is a subgroup of $(\mathbb{Z}, +)$ by Corollary 3.2.7, it follows that $m, n \in G_p$ if and only if $(m, n) \in G_p$. This proves our assertion. □

In particular, we have proved that $S_l(P) \cap S_p(P) = S_1(P)$ if $l, p \in \mathcal{P}$ and $l \neq p$. This will turn out to be an important fact since T_1 will be largely constituted of sets $S_l(P)$ with l prime numbers.
It also follows that $S_l(P) \cup S_p(P) \subseteq S_{lp}(P)$ for $l, p \in \mathcal{P}$. Recall that $p_{l,p}$ was defined as the maximum of $S_{lp}(P) \setminus (S_l(P) \cup S_p(P))$. For the construction of T_2 we will need the fact that $p_{l,p}$ is well-defined (and thus, the difference is non-empty) if $\max\{l, p\}$ is sufficiently large. The proof of this fact will need some preparation. We start with the following lemma:

Lemma 3.2.9. *Let $z \in \hat{E}(\mathcal{M}_p)$ and let $[m]z = z \oplus_F \ldots \oplus_F z$ denote the multiplication-by-m in $\hat{E}(\mathcal{M}_p)$. Let $l \in \mathcal{P}$. Then there are power series $f, g \in \mathbb{Z}_p[\![t]\!]$ with $f(z) = z + (\text{terms of degree} \geq 2)$ and $g(0) = 0$ which fulfill*

$$[l]z = lf(z) + g(z^l).$$

This follows immediately from Proposition 2.3 and Corollary 4.4, Chapter IV in [16], p. 116, 120-121.

Corollary 3.2.10. *Let $z \in \hat{E}(\mathcal{M}_p)$, $z \neq 0$ and $p \in \mathcal{P}$. Then we have that $\mathrm{ord}_p([p]z) > \mathrm{ord}_p(z)$ and $\mathrm{ord}_p([n]z) = \mathrm{ord}_p(z)$ for all $n \geq 1$ with $(p, n) = 1$. If $p \neq 2$, then $\mathrm{ord}_p([p]z) = \mathrm{ord}_p(z) + 1$.*

Proof: Let $l \in \mathcal{P}$. By Lemma 3.2.9 there are power series $f, g \in \mathbb{Z}_p[\![t]\!]$, $f(z) = z + \sum_{n=2}^{\infty} a_n z^n$, $g(z) = \sum_{n=1}^{\infty} b_n z^n$ such that $[l]z = lf(z) + g(z^l)$. If $l = p$, we have that

$$[p]z = z\left(p + p\sum_{n=2}^{\infty} a_n z^{n-1} + \sum_{n=1}^{\infty} b_n z^{pn-1}\right).$$

Therefore, $\mathrm{ord}_p([p]z) > \mathrm{ord}_p(z)$. If $p \neq 2$, then $\mathrm{ord}_p(p\sum_{n=2}^{\infty} a_n z^{n-1} + \sum_{n=1}^{\infty} b_n z^{pn-1}) \geq 2$ and this implies that $\mathrm{ord}_p([p]z) = \mathrm{ord}_p(z) + 1$.
Now suppose that $l \neq p$. Then

$$[l]z = z\left(l + l\sum_{n=2}^{\infty} a_n z^{n-1} + \sum_{n=1}^{\infty} b_n z^{ln-1}\right).$$

Since $\mathrm{ord}_p(l\sum_{n=2}^{\infty} a_n z^{n-1} + \sum_{n=1}^{\infty} b_n z^{ln-1}) \geq 1$, we have that $\mathrm{ord}_p([l]z) = \mathrm{ord}_p(z)$. It follows by induction that $\mathrm{ord}_p([n]z) = \mathrm{ord}_p(z)$ for all $n \geq 1$ with $(p, n) = 1$. □

From this result we can derive how $\mathrm{ord}_p(x(Q))$ and $\mathrm{ord}_p(x(n \cdot Q))$ differ for a point $Q \in E(\mathbb{Q}_p)$ when $p \neq 2$.

Lemma 3.2.11. *Let Q be a point of infinite order in $E_1(\mathbb{Q}_p)$. Then the following statements are true:*

(1) *If $n \geq 1$ with $(p, n) = 1$, then $\mathrm{ord}_p(x(n \cdot Q)) = \mathrm{ord}_p(x(Q))$ and $\mathrm{ord}_p(y(n \cdot Q)) = \mathrm{ord}_p(y(Q))$.*

(2) *If $p \neq 2$, then $\mathrm{ord}_p(x(p \cdot Q)) = \mathrm{ord}_p(x(Q)) - 2$ and $\mathrm{ord}_p(y(p \cdot Q)) = \mathrm{ord}_p(y(Q)) - 3$.*

Proof: By Lemma 3.2.5 there is a $z \in \mathcal{M}_p$ with $[n]z \neq 0$ for all $n \geq 1$ with the property $Q = (x, y) = (\frac{z}{w(z)}, -\frac{1}{w(z)})$. Our first assertion follows from Corollary 3.2.10 since

$$\mathrm{ord}_p(x(n \cdot Q)) = \mathrm{ord}_p\left(\frac{[n]z}{w([n]z)}\right) = \mathrm{ord}_p\left(\frac{z}{w(z)}\right) = \mathrm{ord}_p(x(Q)),$$

$$\operatorname{ord}_p(y(n\cdot Q)) = \operatorname{ord}_p\left(-\frac{1}{w([n]z)}\right) = \operatorname{ord}_p\left(-\frac{1}{w(z)}\right) = \operatorname{ord}_p(y(Q)).$$

Because of (3.2.2), $\operatorname{ord}_p(w(z')) = 3\operatorname{ord}_p(z')$ for all $z' \neq 0$. With Corollary 3.2.10 we conclude that

$$\operatorname{ord}_p(x(Q)) = \operatorname{ord}_p\left(\frac{z}{w(z)}\right) = \operatorname{ord}_p(z) - 3\operatorname{ord}_p(z) = -2\operatorname{ord}_p(z),$$

$$\operatorname{ord}_p(x(p\cdot Q)) = \operatorname{ord}_p\left(\frac{[p]z}{w([p]z)}\right) = \operatorname{ord}_p(z) + 1 - 3(\operatorname{ord}_p(z)+1) = -2\operatorname{ord}_p(z) - 2,$$

$$\operatorname{ord}_p(y(Q)) = \operatorname{ord}_p\left(-\frac{1}{w(z)}\right) = -3\operatorname{ord}_p(z),$$

$$\operatorname{ord}_p(y(p\cdot Q)) = \operatorname{ord}_p\left(-\frac{1}{w([p]z)}\right) = -3\operatorname{ord}_p(z) - 3.$$

Thus, our second assertion holds. □

Corollary 3.2.12. $\operatorname{ord}_p(d_{mn}(P)) = \operatorname{ord}_p(d_n(P)) + 2\operatorname{ord}_p(m)$ *for all* $m, n \geq 1$ *and* $p \in \mathcal{P}$ *with* $p \mid d_n(P)$. *In particular,* $d_n(P) \mid d_{mn}(P)$ *for all* $n, m \geq 1$.

Proof: Since $p \mid d_n(P)$, it follows that $n \cdot P \in E_1(\mathbb{Q}_p)$ and $p \neq 2$. By applying Lemma 3.2.11, we derive that $\operatorname{ord}_p(x_{mn}) = \operatorname{ord}_p(x_n) - 2\operatorname{ord}_p(m)$. This proves our assertion since we have that $\operatorname{ord}_p(x_n) = -\operatorname{ord}_p(d_n(P))$ and $\operatorname{ord}_p(x_{mn}) = -\operatorname{ord}_p(d_{mn}(P))$. □

Next we introduce several height functions. An exhaustive description of these functions (apart from h_0) and their behavior on E can be found in §4 and §5 of Chapter VIII in [16].

Definition 3.2.13 (Height functions)**.** For a point $Q \in \mathbb{P}^n(\mathbb{Q})$ with projective coordinates $Q = (x_0 : \ldots : x_n)$ we define its height as

$$H(Q) := \prod_{v \in \mathcal{P}\cup\{\infty\}} \max\{|x_0|_v, \ldots, |x_n|_v\}.$$

Further, we define the logarithmic height of Q as $h(Q) := \log H(Q)$. For $x \in \mathbb{Z} \setminus \{0\}$ we define

$$h_0(x) := \sum_{v \in S_0(\mathbb{Q})\cup\{\infty\}} \log|x|_v.$$

For $Q \in E(\mathbb{Q})$ we define the canonical height of Q as

$$\hat{h}(Q) := \frac{1}{2}\lim_{n\to\infty} 4^{-n} h(f_x(2^n \cdot Q))$$

where $f_x : \mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$ is the rational function $f_x(x : y : z) := (x/z : 1)$ (so we have that $h(f_x(Q)) = \log x(Q)$ for $Q \neq \mathcal{O}$ and $h(f_x(\mathcal{O})) = 0$).

Lemma 3.2.14. *The following statements are true:*

(1) *Let* $Q = (x_0 : \ldots : x_n) \in \mathbb{P}^n(\mathbb{Q})$ *with* $x_1, \ldots, x_n \in \mathbb{Z}$ *and* $(x_0, \ldots, x_n) = 1$. *Then we have that* $H(Q) = \max\{|x_0|, \ldots, |x_n|\}$.

(2) *Let* $x \in \mathbb{Z} \setminus \{0\}$. *Then* $h_0(x) = -\sum_{p \in \mathcal{P}\setminus S_0(\mathbb{Q})} \log|x|_p$.

(3) $h_0(d_n(P)) = h(d_n(P)) = \log d_n(P)$ *for all* $n \geq 1$. *(Here we treat* $d_n(P)$ *as* $(d_n(P) : 1) \in \mathbb{P}^2(\mathbb{Q})$.*)*

Proof: (1) follows from the fact that $\prod_{p\in\mathcal{P}} \max\{|x_0|_p, \ldots, |x_n|_p\} = 1$ if $(x_0, \ldots, x_n) = 1$.
(2) is an obvious implication of the identity $\prod_{v\in\mathcal{P}\cup\{\infty\}} |x|_v = 1$ for all $x \in \mathbb{Z} \setminus \{0\}$.
Lastly, (3) is a consequence of the fact that $\mathrm{ord}_p(d_n(P)) = 0$ and that $\log |d_n(P)|_p = 0$ for all $p \in S_0(\mathbb{Q})$. □

Lemma 3.2.15. *Let* $x, y \in \mathbb{Z} \setminus \{0\}$. *Then the following statements are true:*

(1) $h_0(xy) = h_0(x) + h_0(y)$.

(2) $x \mid y \Rightarrow h_0(x) \leq h_0(y)$.

Proof: This is obvious from Definition 3.2.13. □

The following two theorems provide us with estimates for the height functions:

Theorem 3.2.16 (Néron-Tate)**.**

(1) $\hat{h}(n \cdot P) = n^2\hat{h}(P)$ *for all* $n \geq 1$.

(2) $\hat{h}(n \cdot P) = h(x_n) + O(1)$ *as* $n \to \infty$.

This is proved in Theorem 9.3, Chapter VIII of [16], p. 229-231.

Theorem 3.2.17 (Serre)**.** $\log |x_n|_v = o(h(x_n))$ *for all* $v \in \mathcal{P} \cup \{\infty\}$ *as* $n \to \infty$.

The proof for this theorem can be found in [14], p. 101.

We now can find an estimate for $h_0(d_n(P))$ which will be our final lemma for proving the existence of $p_{l,p}(P)$.

Lemma 3.2.18. $h_0(d_n(P)) = (\hat{h}(P) + o(1))n^2$ *as* $n \to \infty$.

Proof: We begin with the observation that

$$h(x_n) = \sum_{v\in\mathcal{P}\cup\{\infty\}} \log \max\{|x_n|_v, 1\}$$

$$= \sum_{v\in S_0(\mathbb{Q})\cup\{\infty\}} \log \max\{|x_n|_v, 1\} + \sum_{p\in S_n(P)} \log \max\{|x_n|_p, 1\} + \sum_{p\in\mathcal{P}\setminus(S_0(\mathbb{Q})\cup S_n(P))} \log \max\{|x_n|_p, 1\}.$$

By Theorem 3.2.17 we have that

$$\sum_{v\in S_0(\mathbb{Q})\cup\{\infty\}} \log \max\{|x_n|_v, 1\} = o(h(x_n)).$$

Next we observe that, since $|x_n|_p = \frac{1}{|d_n(P)|_p}$ for all $p \in S_n(P)$ and $|d_n(P)|_p = 1$ for all $p \notin S_n(P)$, we have that

$$\sum_{p\in S_n(P)} \log \max\{|x_n|_p, 1\} = -\sum_{p\in S_n(P)} \log |d_n(P)|_p = -\sum_{p\in\mathcal{P}\setminus S_0(\mathbb{Q})} \log |d_n(P)|_p = h_0(d_n(P))$$

by Lemma 3.2.14 (2).
Finally, since $|x_n|_p \leq 1$ for all $p \in \mathcal{P} \setminus (S_0(\mathbb{Q}) \cup S_n(P))$, we have that

$$\sum_{p \in \mathcal{P} \setminus (S_0(\mathbb{Q}) \cup S_n(P))} \log \max\{|x_p|_v, 1\} = 0.$$

Combining these results, we derive the identity $h_0(d_n(P)) = h(x_n) + o(h(x_n))$. With Theorem 3.2.16 we now can conclude that

$$h_0(d_n(P)) = \hat{h}(P)n^2 + O(1) + o(\hat{h}(P)n^2 + O(1)) = \hat{h}(P)n^2 + o(n^2) = (\hat{h}(P) - o(1))n^2.$$

□

Now we can already prove the second main theorem of this section which will be important for defining T_2:

Theorem 3.2.19. *There is a $L \in \mathbb{R}$ such that for all $l, p \in \mathcal{P}$ with $l > L$ we have that*

$$S_{lp}(P) \setminus (S_l(P) \cup S_p(P)) \neq \emptyset.$$

Thus, $p_{l,p}(P) = p_{p,l}(P)$ is well-defined for sufficiently large $\max\{l, p\}$.

Proof: Suppose that $S_{lp}(P) \setminus (S_l(P) \cup S_p(P)) = \emptyset$. Let $q \in S_{lp}(P)$ and assume, without loss of generality, that $q \in S_l(P)$. By Corollary 3.2.12 we have that $\mathrm{ord}_q(d_{lp}(P)) = \mathrm{ord}_q(d_l(P))$ if $q \neq p$ and $\mathrm{ord}_q(d_{lp}(P)) = \mathrm{ord}_q(d_l(P)) + 2$ if $q = p$.
Thus, we can conclude that $d_{lp}(P) \mid d_l(P)d_p(P)l^2p^2$. It follows from the definition of h_0 that $h_0(l^2) = 0$ if $l \in S_0(\mathbb{Q})$ and $h_0(l^2) = \log l^2 \leq l$ else. Since the same is true for $h_0(p^2)$, it follows with Lemma 3.2.15 that

$$h_0(d_{lp}(P)) \leq h_0(d_l(P)) + h_0(d_p(P)) + l + p. \tag{3.2.4}$$

By Lemma 3.2.18 there is a $c > 0$ such that $h_0(d_n(P)) = (c + o(1))n^2$ as $n \to \infty$. Now let $\varepsilon > 0$ with $c > 3\varepsilon$. There is a $N \in \mathbb{N}$ such that for all $n \geq N$ we have that $h_0(d_n(P)) = (c + o(1))n^2$ with $|o(1)| < \varepsilon$. Also let $C > 0$ be such that $h_0(d_n(P)) < Cn^2$ for all $n \geq 1$. Now we define

$$L := \max\left\{N, \frac{1}{c - 3\varepsilon}, \frac{CN^2 + N + 1}{3c - 5\varepsilon}\right\}.$$

Let $l, p \in \mathcal{P}$ with $l > L$. We consider two cases, $p \geq N$ and $p < N$.
If we suppose that $S_{lp}(P) \setminus (S_l(P) \cup S_p(P)) = \emptyset$, we can derive from (3.2.4) that

$$(c + o(1))l^2p^2 \leq (c + o(1))l^2 + (c + o(1))p^2 + l + p. \tag{3.2.5}$$

If $p \geq N$, it follows that

$$(c - \varepsilon)l^2p^2 < (c + \varepsilon)l^2 + (c + \varepsilon)p^2 + l + p.$$

Dividing both sides of the equation with l^2p^2, we get (with $l, p \geq 2$)

$$c - \varepsilon < (c + \varepsilon)p^{-2} + (c + \varepsilon)l^{-2} + \frac{1}{lp^2} + \frac{1}{l^2p} \leq \frac{c + \varepsilon}{2} + \frac{1}{2l}.$$

Thus, we have $c < 3\varepsilon + \frac{1}{l}$ which is a contradiction to our choice of l.
Now suppose that $p < N$. Then we derive from (3.2.5) that

$$4(c-\varepsilon)l^2 \leq (c-\varepsilon)l^2p^2 \leq (c+\varepsilon)l^2 + CN^2 + N + l.$$

Further, we conclude that

$$(3c-5\varepsilon)l \leq \frac{CN^2+N}{l} + 1 < CN^2 + N + 1$$

which is a contradiction to our choice of l. □

Corollary 3.2.20. *Let $c > 0$ and $l_1, \ldots, l_n \in \mathcal{P}$. Then there is a $N \in \mathbb{N}$ such that for all $p \in \mathcal{P}$ with $p \geq N$, $p_{p,l_i}(P)$ is well-defined and $p_{p,l_i}(P) > c$ for all $i \in \{1, \ldots, n\}$.*

Proof: By Theorem 3.2.19 there is a $L \in \mathbb{R}$ such that $p_{p,l_i}(P)$ is well-defined for $p > L$. Let $(l,p) \neq (l',p')$ be two distinct pairs of prime numbers. Without loss of generality assume that $p \neq p'$. If $l = l'$ then we have with Theorem 3.2.8 that

$$(S_{lp}(P) \setminus (S_l(P) \cup S_p(P))) \cap (S_{lp'}(P) \setminus (S_l(P) \cup S_{p'}(P)))$$

$$\subseteq (S_{lp}(P) \setminus S_l(P)) \cap (S_{lp'}(P) \setminus S_l(P)) = S_{(lp,lp')}(P) \setminus S_l(P) = S_l(P) \setminus S_l(P) = \emptyset.$$

If $l \neq l'$, then $(lp, l'p') = 1$ and therefore

$$(S_{lp}(P) \setminus (S_l(P) \cup S_p(P))) \cap (S_{l'p'}(P) \setminus (S_{l'}(P) \cup S_{p'}(P))) = \emptyset.$$

It follows that $p_{l,p}(P) \neq p_{l',p'}(P)$ if $(l,p) \neq (l',p')$. Thus, there are only finitely many pairs (l,p) of primes numbers with $p_{l,p}(P) \leq c$ and there is a $N \geq L$ with $p_{p,l_i}(P) > c$ for all $p \geq N$ and for all i with $1 \leq i \leq n$. □

The next important result will be that the set $\mathcal{U}(P) := \{p_l(P) | l \in \mathcal{P}\}$ has natural density equal to zero. We will need this for showing that the natural density of T_2 is zero. We require a number of auxiliary results and start with the structure of the subgroup $E(K)[m]$.

Lemma 3.2.21. *Let E be an elliptic curve over an algebraically closed field K and $m \geq 1$. If $\mathrm{Char}(K) = 0$ or $(\mathrm{Char}(K), m) = 1$, then $E(K)[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$.*

This is proved in Corollary 6.4, Chapter III of [16], p. 89-90.

Lemma 3.2.22. *Let K be a finite extension of $\mathbb{Q}$, $\mathfrak{p}$ a prime of K and $m \geq 1$ with $\mathrm{ord}_{\mathfrak{p}}(m) = 0$. Let E be an elliptic curve over K. If the reduced curve $E(\mathbb{F}_{\mathfrak{p}})$ is non-singular, the reduction map $\pi_{\mathfrak{p}} : E(K_{\mathfrak{p}}) \to E(\mathbb{F}_{\mathfrak{p}})$ restricted to $E(K_{\mathfrak{p}})[m]$ is injective.*

This is Proposition 3.1(b), Chapter VII in [16], p. 176.

Corollary 3.2.23. *Let K be a finite extension of $\mathbb{Q}$, $\mathfrak{p} \notin S_0(K)$ and $m \geq 1$ with $\mathrm{ord}_{\mathfrak{p}}(m) = 0$. If $E(K)[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$, then $E(K)[m] \cong E(\overline{\mathbb{F}_{\mathfrak{p}}})[m]$ and reduction modulo $\mathfrak{p}$ induces an isomorphism.*

Proof: By Lemma 3.2.21 we have that $E(\overline{\mathbb{F}_{\mathfrak{p}}})[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$ since $\mathrm{ord}_{\mathfrak{p}}(m) = 0$. Further, the map $\pi_{\mathfrak{p}} : E(K_{\mathfrak{p}})[m] \to E(\mathbb{F}_{\mathfrak{p}})[m] \subseteq E(\overline{\mathbb{F}_{\mathfrak{p}}})[m]$ is injective by Lemma 3.2.22 since $\mathfrak{p} \notin S_0(K)$. Therefore,

the map $\pi_{\mathfrak{p}}|_{E(K)[m]}$ is also injective. Now the assertion follows with

$$\#\pi(E(K)[m]) = m^2 = \#E(\overline{\mathbb{F}_{\mathfrak{p}}})[m].$$

□

The first important property of $\mathcal{U}(P)$, that we will prove, is that $l \mid \#E(\mathbb{F}_{p_l(P)})$ for all $l \in \mathcal{P}$.

Lemma 3.2.24. *Let $l, p \in \mathcal{P}$. If $p \in S_{l^{a_l(P)}}(P) \setminus S_1(P)$, then $l \mid \#E(\mathbb{F}_p)$.*

Proof: Since $p \notin S_0(\mathbb{Q})$, the curve $E(\mathbb{F}_p)$ is non-singular. If $Q = (\frac{a}{b^2} : \frac{c}{b^3} : 1) = (ab : c : b^3)$ with $a, b, c \in \mathbb{Z}$ and $(ac, b) = 1$ is an arbitrary point $Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, it is obvious that

$$\pi_p(Q) = (0 : 1 : 0) = \tilde{\mathcal{O}} \iff \mathrm{ord}_p(b) > 0.$$

But since $p \in S_{l^{a_l(P)}}(P) \setminus S_1(P)$ and $S_{l^i}(P) = S_1(P)$ for $1 \leq i < a_l(P)$ by the definition of $a_l(P)$, we know that $\mathrm{ord}_p(x_{l^{a_l(P)}}) < 0$ and $\mathrm{ord}_p(x_{l^i}) \geq 0$ for $1 \leq i < a_l(P)$. Thus, $\pi_p(P)$ is an element of order $l^{a_l(P)}$ of $E(\mathbb{F}_p)$ and $l \mid \#E(\mathbb{F}_p)$. □

By a well-known result from group theory we have that $l \mid \#E(\mathbb{F}_p)$ if and only if $E(\mathbb{F}_p)$ has an element of order l. Therefore, we will give a condition when $E(\mathbb{F}_p)$ has an element of order l in the next theorem. Beforehand, we will introduce the notion of the Frobenius automorphism for an unramified prime.

Lemma 3.2.25 (Frobenius automorphism for $\mathfrak{p}$)**.** *Let K be a finite, normal extension of $\mathbb{Q}$ and $\mathfrak{p}$ an unramified prime of K lying over a prime p of $\mathbb{Q}$.*
Let $\tau \in \mathrm{Gal}(K/\mathbb{Q})$. Then $\tau|_{\mathcal{O}_K} : \mathcal{O}_K \to \mathcal{O}_K$ is a ring automorphism and $\overline{\tau|_{\mathcal{O}_K}} : \mathcal{O}_K/\mathfrak{p} \to \mathcal{O}_K/\mathfrak{p}$ is an automorphism such that the diagram

$$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{\tau|_{\mathcal{O}_K}} & \mathcal{O}_K \\ {\scriptstyle \pi_{\mathfrak{p}}}\downarrow & & \downarrow{\scriptstyle \pi_{\mathfrak{p}}} \\ \mathcal{O}_K/\mathfrak{p} & \xrightarrow{\overline{\tau|_{\mathcal{O}_K}}} & \mathcal{O}_K/\mathfrak{p} \end{array}$$

is commutative. The following statements are true:

- *The subgroup $\{\tau \in \mathrm{Gal}(K/\mathbb{Q}) | \tau(\mathfrak{p}) = \mathfrak{p}\} \subseteq \mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to the group*

  $$\mathrm{Gal}((\mathcal{O}_K/\mathfrak{p})/(\mathbb{Z}/p)) = \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$$

  via the map $\tau \mapsto \overline{\tau|_{\mathcal{O}_K}}$.

- *$\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ is a cyclic group and is generated by the automorphism $s(x) := x^p$. Thus, there is a unique automorphism $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma_{\mathfrak{p}}(x) \equiv x^p \pmod{\mathfrak{p}}$ for all $x \in \mathcal{O}_K$ and $\sigma_{\mathfrak{p}}$ generates the subgroup $\{\tau \in \mathrm{Gal}(K/\mathbb{Q}) | \tau(\mathfrak{p}) = \mathfrak{p}\}$ of $\mathrm{Gal}(K/\mathbb{Q})$. In particular, the following diagram is commutative:*

  $$\begin{array}{ccc} \mathcal{O}_K & \xrightarrow{\sigma_{\mathfrak{p}}} & \mathcal{O}_K \\ {\scriptstyle \pi_{\mathfrak{p}}}\downarrow & & \downarrow{\scriptstyle \pi_{\mathfrak{p}}} \\ \mathcal{O}_K/\mathfrak{p} & \xrightarrow{x \mapsto x^p} & \mathcal{O}_K/\mathfrak{p} \end{array}$$

The map $\sigma_{\mathfrak{p}}$ is called the Frobenius automorphism for $\mathfrak{p}$.
If $p \in \mathcal{P}$ is a prime number that is unramified in the extension $K/\mathbb{Q}$, the set

$$\{\sigma_{\mathfrak{p}} | \mathfrak{p} \text{ lies over } p\} \subseteq \mathrm{Gal}(K/\mathbb{Q})$$

is invariant under conjugation.

See section 7.3 of [9] for an exhaustive discussion of the Frobenius automorphism for an unramified prime.

Theorem 3.2.26. *Let $l, p \in \mathcal{P}$, $l \neq p$. Let M be a finite Galois extension of $\mathbb{Q}$ such that $E(\overline{\mathbb{Q}})[l] \setminus \{\mathcal{O}\} \subseteq M^2$. Assume that $\mathfrak{p} \notin S_0(M)$ for all primes $\mathfrak{p}$ of M that are factors of p. Then $E(\mathbb{F}_p)$ has an element of order l if and only if there is a $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ and a point $Q \in E(\overline{\mathbb{Q}})[l] \setminus \{\mathcal{O}\}$ with $\sigma(Q) = Q$ and σ is the Frobenius automorphism for some factor $\mathfrak{p}$ of p.*

Proof: First assume that there is a $\tilde{Q} \in E(\mathbb{F}_p)[l] \setminus \{\tilde{\mathcal{O}}\}$. Let $\mathfrak{p}$ be any prime of M over p. Since $\mathbb{F}_p \subseteq \mathbb{F}_{\mathfrak{p}} \subseteq \overline{\mathbb{F}_{\mathfrak{p}}}$, we have that $\tilde{Q} \in E(\overline{\mathbb{F}_{\mathfrak{p}}})[l]$. Since we have that $E(M)[l] = E(\overline{\mathbb{Q}})[l] \cong (\mathbb{Z}/l\mathbb{Z})^2$ by Lemma 3.2.21, the conditions of Corollary 3.2.23 are fulfilled and $E(\overline{\mathbb{F}_{\mathfrak{p}}})[l] \cong E(M)[l]$. Thus, there is a $Q \in E(M)[l] = E(\overline{\mathbb{Q}})[l]$, $Q \neq \mathcal{O}$ with $\pi_{\mathfrak{p}}(Q) = \tilde{Q}$. Since $\mathfrak{p} \notin S_0(M)$, $\mathfrak{p}$ is unramified over $\mathbb{Q}$ and by Lemma 3.2.25, the Frobenius automorphism σ for $\mathfrak{p}$ exists. Suppose that $\sigma(Q) \neq Q$. This would imply that $Q^p \not\equiv Q \pmod{\mathfrak{p}}$. Consequently, we would have that $\tilde{Q} = \pi_{\mathfrak{p}}(Q) \notin E(\mathbb{F}_p)$ which is a contradiction to our assumption.
Now suppose that there is a $Q \in E(M)[l] \setminus \{\mathcal{O}\}$ with $\sigma(Q) = Q$ and σ is the Frobenius automorphism for some factor $\mathfrak{p}$ of p. Thus, $Q^p \equiv Q \pmod{\mathfrak{p}}$. Let $\tilde{Q} := \pi_{\mathfrak{p}}(Q) \in E(\mathbb{F}_{\mathfrak{p}})$. Then we have that $\tilde{Q}^p = \tilde{Q}$ and $\tilde{Q} \in E(\mathbb{F}_p)$. Since $\pi_{\mathfrak{p}}$ is an injective homomorphism on $E(M)[l]$, it is obvious that $\tilde{Q}$ is an element of order l of $E(\mathbb{F}_p)$. □

The next two lemmata will provide us with estimates which we will use in our proof of $\delta_{nat}(\mathcal{U}(P)) = 0$.

Lemma 3.2.27. *Let K be a finite extension of $\mathbb{Q}$ and $l \in \mathcal{P}$. Then $\mathrm{Aut}(E(\overline{K})[l]) \cong \mathrm{GL}_2(\mathbb{F}_l)$ where $E(\overline{K})[l]$ is treated as a 2-dimensional vector space over $\mathbb{F}_l$. Further, let*

$$n_l := \frac{\#\{\sigma \in \mathrm{Aut}(E(\overline{K})[l]) | \exists Q \in E(\overline{K})[l] \setminus \{\mathcal{O}\}, \sigma(Q) = Q\}}{\#\,\mathrm{Aut}(E(\overline{K})[l])}.$$

Then $n_l = \frac{1}{l} + \frac{1}{l^2} + o(\frac{1}{l^2})$ as $l \to \infty$.

Proof: $\mathrm{Aut}(E(\overline{K})[l]) \cong \mathrm{GL}_2(\mathbb{F}_l)$ is obvious from Lemma 3.2.21. Now we want to determine the number of 2×2-matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_l)$$

which fix a non-zero vector in $\mathbb{F}_l^2$. Thus, we search for all 4-tuples $(a, b, c, d) \in \mathbb{F}_l^4$ which satisfy

$$(a-1)(d-1) - bc = 0 \ \wedge \ ad - bc \neq 0.$$

This can be simplified to

$$a + d \neq 1 \wedge bc = (a-1)(d-1). \tag{3.2.6}$$

$a+d \neq 1$ is true for $l(l-1)$ pairs $(a,d) \in \mathbb{F}_l^2$ (for each choice of $a \in \mathbb{F}_l$ there are $l-1$ possible choices for d). Next we want to count for how many of these pairs (a,d) we have that $(a-1)(d-1)=0$. Altogether there are $2l-1$ pairs $(a,d) \in \mathbb{F}_l^2$ with $(a-1)(d-1)=0$ (namely $(a,1)$, $(1,d)$ and $(1,1)$ with $a,d \in \mathbb{F}_l$ arbitrary). Two of these pairs do not fulfill he condition $a+d \neq 1$ (the pairs $(0,1)$ and $(1,0)$) which leaves us with $2l-3$ pairs (a,d) with $a+d \neq 1$ and $(a-1)(d-1)=0$. For each of these pairs (a,d) there are $2l-1$ pairs $(b,c) \in \mathbb{F}_l^2$ that fulfill the condition $bc=0=(a-1)(d-1)$ (namely $(b,0)$, $(0,c)$ and $(0,0)$ with $b,c \in \mathbb{F}_l$).
Now we consider the remaining $l(l-1)-(2l-3)=l^2-3l+3$ pairs (a,d) with $a+d \neq 1$ and $(a-1)(d-1) \neq 0$. For each of these pairs there are $l-1$ pairs $(b,c) \in \mathbb{F}_l^2$ which fulfill $(a-1)(d-1)=bc$ (if $b \in \mathbb{F}_l^*$ is chosen arbitrarily, c is given by $c=b^{-1}(a-1)(d-1)$).
Altogether there are $(2l-3)(2l-1)+(l^2-3l+3)(l-1)=l(l^2-2)$ 4-tuples $(a,b,c,d) \in \mathbb{F}_l^4$ which fulfill (3.2.6).
Next, we want to compute the size of $\mathrm{GL}_2(\mathbb{F}_l)$. For this we determine the number of all 4-tuples $(a,b,c,d) \in \mathbb{F}_l^4$ which fulfill $ad-bc=0$. We consider the two cases $a=0$ and $a \neq 0$. If $a=0$, we can choose an arbitrary $d \in \mathbb{F}_l$ together with one of $2l-1$ pairs (b,c) (namely $(b,0)$, $(0,c)$ and $(0,0)$) such that $ad-bc=0$ is fulfilled. If $a \neq 0$, then we can take an arbitrary pair $(b,c) \in \mathbb{F}_l^2$ and d is uniquely determined as $d=a^{-1}bc$. In total, we have $l(2l-1)+(l-1)l^2=l^3+l^2-l$ tuples with $ad-bc=0$ which implies that $\#\,\mathrm{GL}_2(\mathbb{F}_l)=l^4-(l^3+l^2-l)=(l^2-l)(l^2-1)$.
Now we can conclude that

$$n_l=\frac{l(l^2-2)}{(l^2-l)(l^2-1)}=\frac{1}{l}+\frac{1}{l^2}-\frac{1}{l^5-l^4-l^3+l^2}=\frac{1}{l}+\frac{1}{l^2}+o\left(\frac{1}{l^2}\right).$$

□

Lemma 3.2.28. *Suppose that the real sequence $\{\alpha_i | i \geq 1\} \subseteq (0,1)$ has the following properties:*

- $\sum_{i=1}^{\infty} \alpha_i = \infty$.
- $\sum_{i=1}^{\infty} \alpha_i^2 < \infty$.
- *There is a $N \in \mathbb{N}$ such that $0 < \alpha_i < \frac{1}{2}$ for all $i \geq N$.*
- $\alpha_{i+1} < \alpha_i$ *for all* $i \geq 1$.

Further, define $S(n) := \sum_{i=1}^{n} \alpha_i$ and $G(n) := \prod_{i=1}^{n}(1-\alpha_i)$ for $n \geq 1$. Then the following statements are true:

(1) $G(n) = O(1)e^{-S(n)}$ *as* $n \to \infty$.

(2) *For all $k \geq 1$ we have that*

$$\lim_{n\to\infty} G(n) \sum_{1 \leq i_1 < \ldots < i_k \leq n} \frac{\alpha_{i_1} \cdots \alpha_{i_k}}{(1-\alpha_{i_1}) \cdots (1-\alpha_{i_k})} = 0.$$

Proof of (1): We have that

$$\log G(n) = \sum_{i=1}^{n} \log(1-\alpha_i) = -S(n) + \sum_{i=1}^{n} (\alpha_i + \log(1-\alpha_i)).$$

Since $|x+\log(1-x)| \leq x^2$ for all $x \in (0, \frac{1}{2})$, it follows from the properties of $(\alpha_i)_{i\geq 1}$ that

$$\left|\sum_{i=1}^{n}(\alpha_i+\log(1-\alpha_i))\right| \leq \sum_{i=1}^{N}|\alpha_i+\log(1-\alpha_i)| + \sum_{i=N+1}^{n}\alpha_i^2 < \sum_{i=1}^{N}|\alpha_i+\log(1-\alpha_i)| + \sum_{i=1}^{\infty}\alpha_i^2$$

for all $n \geq 1$. Thus, we have that $\log G(n) = -S(n) + O(1)$ and $G(n) = O(1)e^{-S(n)}$.
Proof of (2): Let $k \geq 1$. Then we have that

$$G(n)\sum_{1\leq i_1<\ldots<i_k\leq n}\frac{\alpha_{i_1}\cdots\alpha_{i_k}}{(1-\alpha_{i_1})\cdots(1-\alpha_{i_k})} \leq G(n)(1-\alpha_1)^{-k}\sum_{i_1=1}^{n}\cdots\sum_{i_k=1}^{n}\alpha_{i_1}\cdots\alpha_{i_k}$$

$$= O(1)e^{-S(n)}(1-\alpha_1)^{-k}(S(n))^k \to 0$$

as $n \to \infty$. □

The next important ingredient, which we will use for showing $\delta_{nat}(\mathcal{U}(P)) = 0$, is the Galois action on the torsion group of $E(\overline{\mathbb{Q}})$:

Lemma 3.2.29. *Let $n \geq 1$. Then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the group $E(\overline{\mathbb{Q}})[n]$ by $\sigma(Q) := (\sigma(x(Q)), \sigma(y(Q)))$ for $Q \neq \mathcal{O}$ and $\sigma(\mathcal{O}) := \mathcal{O}$. Thus, there is a group homomorphism $\Lambda_n : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(\overline{\mathbb{Q}})[n])$.*

For a discussion of this homomorphism see §7, Chapter III of [16].
This group action obviously implies a group homomorphism

$$\Lambda_\infty : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T(E(\overline{\mathbb{Q}})))$$

where $T(E(\overline{\mathbb{Q}}))$ is the torsion group of $E(\overline{\mathbb{Q}})$. For this homomorphism we have the following result of Jean-Pierre Serre (which uses as a requirement that E does not have complex multiplication):

Theorem 3.2.30 (Serre)**.** *There is a $m \geq 1$ such that $\Lambda_\infty(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ contains all automorphisms of $T(E(\overline{\mathbb{Q}}))$ whose restriction to $E(\overline{\mathbb{Q}})[m]$ is the identity.*

This is assertion (3) on p. 260 of [12]. It follows that there is a finite set $S(\mathbb{Q}) \subseteq \mathcal{P}$ such that the group homomorphism

$$\Lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \prod_{l\in\mathcal{P}\setminus S(\mathbb{Q})}\mathrm{Aut}(E(\overline{\mathbb{Q}})[l])$$

is surjective.

Theorem 3.2.31 (Cheboratev density theorem)**.** *Let K be a Galois extension of $\mathbb{Q}$ with $[K:\mathbb{Q}] = n$ and let $A \subseteq \mathrm{Gal}(K/\mathbb{Q})$ be a conjugacy class. Let P_A be the set of prime numbers p which are unramified in the extension and for which the Frobenius automorphism $\sigma_{\mathfrak{p}}$ is an element of A for one (and thus for all) primes $\mathfrak{p}$ of K lying over p. Then we have that*

$$\delta_{nat}(P_A) = \frac{\#A}{n}.$$

This is Theorem 1 of [13], p. 331.
The next theorem is the main technical preparation we need for showing $\delta_{nat}(\mathcal{U}(P)) = 0$.

Theorem 3.2.32. *We define for $p \in \mathcal{P} \setminus S_0(\mathbb{Q})$, $t \geq 1$ and $C > 0$:*

$$\mathcal{A}(p, C) := \{l \in \mathcal{P} \setminus S(\mathbb{Q}) : l \mid \#E(\mathbb{F}_p), l < C\},$$

$$f(p, C) := \#\mathcal{A}(p, C),$$

$$\mathcal{B}(C, t) := \{p \in \mathcal{P} \setminus S_0(\mathbb{Q}) | f(p, C) \leq t\}.$$

Then we have for every $t \geq 1$ that

$$\lim_{C \to \infty} \delta_{nat}^{up}(\mathcal{B}(C, t)) = 0.$$

Proof: For $C > 0$ define M_C to be a finite Galois extension of $\mathbb{Q}$ with the property that $E(\overline{\mathbb{Q}})[l] \setminus \{\mathcal{O}\} \subseteq M_C^2$ for all prime numbers $l \leq C$. By Theorem 3.2.30 we know that the group homomorphism

$$\Lambda_C : \mathrm{Gal}(M_C/\mathbb{Q}) \to \prod_{l \in \mathcal{P} \setminus S(\mathbb{Q}), l \leq C} \mathrm{Aut}(E(\overline{\mathbb{Q}})[l]) =: H_C$$

is surjective. Let $\{l_1, \ldots, l_n\} = \{l \in \mathcal{P} \setminus S(\mathbb{Q}) | l \leq C\}$. Now we define for $t \geq 1$:

$$\Sigma(C, t) := \{\sigma \in \mathrm{Gal}(M_C/\mathbb{Q}) | \Lambda_C(\sigma) \text{ has at most } t \text{ components with a fixed point } Q \neq \mathcal{O}\},$$

$$R(C, t) := \frac{\#\Sigma(C, t)}{\#\,\mathrm{Gal}(M_C/\mathbb{Q})}.$$

Since Λ_C is a surjective homomorphism, we have that:

$$R(C, t) = \frac{\#\{\tau \in H_C | \tau \text{ has at most } t \text{ components with a fixed point } Q \neq \mathcal{O}\}}{\#H_C}$$

For $j \in \{1, \ldots, n\}$ and $I_j \subseteq \{1, \ldots, n\}$ with $\#I_j = j$ we define:

$$F_{I_j} := \{(\tau_1, \ldots, \tau_n) \in H_C | \forall i \in I_j \exists Q \in E(\overline{\mathbb{Q}})[l_i] \setminus \{\mathcal{O}\} : \tau_i(Q) = Q\},$$

$$G_{I_j} := \{(\tau_1, \ldots, \tau_n) \in H_C | \forall i \notin I_j \forall Q \in E(\overline{\mathbb{Q}})[l_i] \setminus \{\mathcal{O}\} : \tau_i(Q) \neq Q\}.$$

Further, we define for $i \in \{1, \ldots, n\}$,

$$\alpha_i := \frac{\#\{\tau \in \mathrm{Aut}(E(\overline{\mathbb{Q}})[l_i]) | \exists Q \in E(\overline{\mathbb{Q}})[l_i] \setminus \{\mathcal{O}\} : \tau(Q) = Q\}}{\#\,\mathrm{Aut}(E(\overline{\mathbb{Q}})[l_i])}.$$

Then we have that

$$R(C, t) = \sum_{j=1}^{t} \sum_{I_j} \frac{\#(F_{I_j} \cap G_{I_j})}{\#H_C} = \sum_{j=1}^{t} \sum_{I_j} \Big(\prod_{i \in I_j} \alpha_i \Big) \Big(\prod_{i \notin I_j} (1 - \alpha_i) \Big)$$

$$= \sum_{j=1}^{t} \sum_{I_j} \Big(\prod_{i \in I_j} \frac{\alpha_i}{1 - \alpha_i} \Big) \Big(\prod_{i=1}^{n} (1 - \alpha_i) \Big).$$

Notice that we have $\alpha_i = 1/l_i + 1/l_i^2 + o(1/l_i^2)$ by Lemma 3.2.27. Therefore, the requirements of Lemma 3.2.28 are fulfilled (after maybe re-ordering a finite number of α_i to secure that $\alpha_{i+1} < \alpha_i$ is fulfilled) and we can conclude that for $t \geq 1$ we have that $R(C,t) \to 0$ as $C \to \infty$ (or equivalently, $n \to \infty$).
Now let $t \geq 1$ and $\varepsilon > 0$. Then we can choose a $C > 0$ such that $R(C,t) < \varepsilon$. Now we want to show $\delta_{nat}^{up}(\mathcal{B}(C,t)) \leq R(C,t)$.
We start by observing that $\Sigma(C,t)$ is closed under conjugation. This is true since we have for $\sigma, \tau \in \mathrm{Gal}(M_C/\mathbb{Q})$ and $Q \in E(M_C)$ that

$$\sigma(Q) = Q \iff (\tau^{-1} \circ \sigma \circ \tau)(\tau^{-1}(Q)) = \tau^{-1}(Q).$$

It follows by Theorem 3.2.31 that the natural density of the set of prime numbers which are unramified in the extension and whose factors have a Frobenius automorphism in $\Sigma(C,t)$ is equal to $R(C,t)$.
Now let $p \in \mathcal{B}(C,t)$ with $\mathfrak{p} \notin S_0(M_C)$ for all factors $\mathfrak{p}$ of p. We consider two cases: $p \nmid \#E(\mathbb{F}_p)$ and $p \mid \#E(\mathbb{F}_p)$. In the first case it follows from the definition of $\mathcal{B}(C,t)$ that there is a $k \leq t$ and a set of prime numbers $\{l_1, \cdots, l_k\} \subseteq \mathcal{P} \setminus S(\mathbb{Q})$ with $l_i \neq p$, $l_i \leq C$ and $l_i \mid \#E(\mathbb{F}_p)$ ($\iff$ $E(\mathbb{F}_p)$ has an element of order l_i) for all $i \in \{1, \ldots, k\}$. Now it follows from Theorem 3.2.26 that there are factors $\mathfrak{p}_i$ of p such that the Frobenius automorphism $\sigma_{\mathfrak{p}_i}$ fixes a point $Q_i \in E(\overline{\mathbb{Q}})[l_i] \setminus \{\mathcal{O}\}$ for all $i \in \{1, \ldots, k\}$. Therefore, p has a factor in M_C with a Frobenius automorphism σ such that $\Lambda_C(\sigma)$ has less then or equal to t components with a fixed point $Q \neq \mathcal{O}$. Thus, $\sigma \in \Sigma(C,t)$.
Similarly, if $p \mid \#E(\mathbb{F}_p)$, there is a $k < t$ such that there are k prime numbers l with $l \notin S(\mathbb{Q})$, $l \neq p$, $l \leq C$ and $l \mid \#E(\mathbb{F}_p)$. Theorem 3.2.26 does not cover the case $l = p$, so it could be that $\sigma \in \Sigma(C, t-1)$. But since $\Sigma(C,t-1) \subseteq \Sigma(C,t)$, we still reach the same conclusion.
All in all, we have shown that $\mathcal{B}(C,t) \setminus \{p \in \mathcal{P} | p \text{ has a factor in } S_0(M)\}$ is contained in the set of prime numbers which are unramified in the extension and whose factors have a Frobenius automorphism in $\Sigma(C,t)$. But since $S_0(M_C)$ is a finite set we can conclude that

$$\delta_{nat}^{up}(\mathcal{B}(C,t)) < \varepsilon$$

for sufficiently large C. □

Utilizing the following two famous results, we can finally prove that the natural density of $\mathcal{U}(P)$ is equal to zero.

Theorem 3.2.33 (Hasse)**.** *Let $p \in \mathcal{P}$ be a prime number such that $E(\mathbb{F}_p)$ is non-singular. Then*

$$|\#E(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}.$$

This is a special case of Theorem 1.1, Chapter V of [16], p. 131.

Theorem 3.2.34 (Prime number theorem)**.**

$$\pi_{\mathbb{Q}}(n) = \frac{n}{\log n} + o\Big(\frac{n}{\log n}\Big) \text{ as } n \to \infty.$$

A proof for this well-known theorem can be found, for example, in [6], Theorem 4, XV, p. 315.

Theorem 3.2.35. *Let* $\mathcal{U}(P) := \{p_l(P) | l \in \mathcal{P}\}$. *Then* $\delta_{nat}(\mathcal{U}(P)) = 0$.

Proof: Let $\varepsilon > 0$. Choose a $t \in \mathbb{N}$ with $2^{2-t} < \frac{\varepsilon}{2}$. By Theorem 3.2.32 there is a $C > 0$ such that $\delta_{nat}^{up}(\mathcal{B}(C,t)) < \frac{\varepsilon}{2}$. Next we want to determine the upper natural density of the set

$$\mathcal{U}(P) \setminus \mathcal{B}(C,t) = \{p_l(P) | l \in \mathcal{P}, f(p_l(P), C) > t\}.$$

Suppose that $l \in \mathcal{P}$ and $p_l(P) \notin \mathcal{B}(C,t)$. By definition of $p_l(P)$ and Lemma 3.2.24 we have that $l \mid \#E(\mathbb{F}_{p_l(P)})$. Since $f(p_l(P), C) > t$, there are at least t other primes which divide $\#E(\mathbb{F}_{p_l(P)})$. Therefore, $2^t l \leq \#E(\mathbb{F}_{p_l(P)})$. By Theorem 3.2.33 we have that

$$\#E(\mathbb{F}_{p_l(P)}) \leq p_l(P) + 1 + 2\sqrt{p_l(P)} < 4p_l(P).$$

Thus, $l < 2^{2-t} p_l(P) < \frac{\varepsilon p_l(P)}{2}$ by our choice of t. This means that for every $p_l(P) \notin \mathcal{B}(C,t)$ there is a distinct prime number $l \in \mathcal{P}$ with $l < \frac{\varepsilon p_l(P)}{2}$. With Theorem 3.2.34 it follows that

$$\#\{p_l(P) | l \in \mathcal{P}, p_l(P) \notin \mathcal{B}(C,t), p_l(P) \leq n\} \leq \#\{l \in \mathcal{P} | l \leq (\varepsilon n)/2\} = \pi_{\mathbb{Q}}\left(\frac{\varepsilon n}{2}\right)$$

$$= \frac{\varepsilon n}{2 \log \frac{1}{2}\varepsilon n} + o\left(\frac{n}{\log n}\right)$$

as $n \to \infty$. Thus, $\delta_{nat}^{up}(\mathcal{U}(P) \setminus \mathcal{B}(C,t)) \leq \frac{\varepsilon}{2}$. But then it follows that

$$\delta_{nat}(\mathcal{U}(P)) \leq \delta_{nat}^{up}(\mathcal{B}(C,t)) + \delta_{nat}^{up}(\mathcal{U}(P) \setminus \mathcal{B}(C,t)) < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

Since ε was chosen arbitrarily, this proves our assertion. □

The last result which we will derive in this section determines the natural density of the set $\{l \in \mathcal{P} | \mu_l(P) > \varepsilon\}$ for an arbitrary $\varepsilon > 0$. We need the following technical lemma:

Lemma 3.2.36. *Let* $(z_n)_{n \geq 1}$ *be a sequence of positive real numbers such that there is a* $C > 0$ *with*

$$z_n < Cn^2 \log z_n \ \forall n \geq 1.$$

Then there is a $c > 0$ *such that*

$$z_n < cn^2 \log n \ \forall n \geq 1.$$

Proof: There is a $\bar{C} > 0$ with $z_n < Cn^2 \log z_n < \bar{C} n^2 \sqrt{z_n}$ for all $n \geq 1$. It follows that $z_n < \bar{C}^2 n^4$. Now we have that

$$\frac{z_n}{n^2 \log n} \leq \frac{Cn^2 \log z_n}{n^2 \log n} \leq \frac{C \log(Cn^2 \log z_n)}{\log n} = \frac{C \log(Cn^2)}{\log n} + \frac{C \log \log z_n}{\log n}$$

$$\leq 2C + \frac{C \log C}{\log n} + \frac{C \log \log(\bar{C}^2 n^4)}{\log n} \to 0$$

as $n \to \infty$ which proves our assertion. □

Theorem 3.2.37. *Let $\varepsilon > 0$. Then $\delta_{nat}(\{l \in \mathcal{P} | \mu_l(P) > \varepsilon\}) = 0$.*

Proof: For every $l \in \mathcal{P}$ with $\mu_l(P) > \varepsilon$ there is a $z_l \in \mathbb{Z}$, $z_l \geq 2$ such that

$$\frac{\#\{p \in S_l(P) \setminus S_1(P) | p \leq z_l\}}{\pi_{\mathbb{Q}}(z_l)} > \varepsilon. \tag{3.2.7}$$

For every $M \in \mathbb{Z}$, $M \geq 2$ we define

$$U_M := \{l \in \mathcal{P} | \mu_l(P) > \varepsilon, M \leq z_l < 2M\}.$$

If $l \in U_M$, it follows with (3.2.7) that

$$\#\{p \in S_l(P) \setminus S_1(P) | p \leq 2M\} \geq \#\{p \in S_l(P) \setminus S_1(P) | p \leq z_l\} > \varepsilon \pi_{\mathbb{Q}}(z_l) \geq \varepsilon \pi_{\mathbb{Q}}(M).$$

By Lemma 3.2.8 we have that $S_p(P) \cap S_l(P) = S_1(P)$ for $p, l \in \mathcal{P}$, $p \neq l$. It follows that

$$\pi_{\mathbb{Q}}(2M) \geq \sum_{l \in U_M} \#\{p \in S_l(P) \setminus S_1(P) | p \leq 2M\} \geq \varepsilon \pi_{\mathbb{Q}}(M) \# U_M.$$

With Theorem 3.2.34 it follows that $\# U_M \leq \frac{\pi_{\mathbb{Q}}(2M)}{\varepsilon \pi_{\mathbb{Q}}(M)} = O(1)$ as $M \to \infty$. Now let $N, k \geq 1$ with $2^{k-1} \leq N < 2^k$. Then we have that

$$\begin{aligned} \#\{l \in \mathcal{P} | \mu_l(P) > \varepsilon, z_l \leq N\} &\leq \sum_{1 \leq i < k} \#\{l \in \mathcal{P} | \mu_l(P) > \varepsilon, 2^i \leq z_l < 2^{i+1}\} \\ &= \sum_{1 \leq i < k} \# U_{2^i} = O(k) = O(\log N). \end{aligned} \tag{3.2.8}$$

But if $\mu_l(P) > \varepsilon$, then it follows with (3.2.7), Lemma 3.2.14 (1)+(3) and Theorem 3.2.18 that

$$\pi_{\mathbb{Q}}(z_l) < \frac{\#(S_l(P) \setminus S_1(P))}{\varepsilon} \leq \frac{\log_2 d_l(P)}{\varepsilon} = \frac{h(d_l(P))}{\varepsilon \log 2} = \frac{h_0(d_l(P))}{\varepsilon \log 2} = O(l^2).$$

By Theorem 3.2.34 we have that $\pi_{\mathbb{Q}}(z_l) = \frac{z_l}{\log z_l} + o(\frac{z_l}{\log z_l})$. It follows that there is a $C > 0$ such that for all l with $\mu_l(P) > \varepsilon$ we have that

$$z_l \left(1 + \frac{o(\frac{z_l}{\log z_l})}{\frac{z_l}{\log z_l}}\right) < C l^2 \log z_l.$$

Thus, there is a $\tilde{C}$ such that $z_l < \tilde{C} l^2 \log z_l$ for all l with $\mu_l(P) > \varepsilon$. By Lemma 3.2.36 there is also a $\bar{C}$ such that $z_l < \bar{C} l^2 \log l$ for all l with $\mu_l(P) > \varepsilon$. Together with (3.2.8) we derive that for $n \geq 1$

$$\begin{aligned} \#\{l \in \mathcal{P} | \mu_l(P) > \varepsilon, l \leq n\} &\leq \#\{l \in \mathcal{P} | \mu_l(P) > \varepsilon, z_l \leq \bar{C} n^2 \log n\} \\ &= O(\log(n^2 \log n)) = o(\pi_{\mathbb{Q}}(n)) \end{aligned}$$

as $n \to \infty$ which proves our assertion. □

3.3 Construction of T_1 and T_2

In this section we will prove the existence and computability of a certain set of prime numbers $\{l_i | i \geq 1\}$ from which T_1 and T_2 will be constructed. Before we can do that, we will need to make sure that there are always sufficiently many prime numbers with $|y_l - l| < \varepsilon$ for an arbitrary $\varepsilon > 0$. We will utilize the following result of Ivan Matveyevich Vinogradov:

Theorem 3.3.1 (Vinogradov)**.** *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Let $J \subseteq [0,1]$ be an interval. Then the natural density of $\{l \in \mathcal{P} | (l\alpha \bmod \mathbb{Z}) \in J\}$ is equal to the length of J.*

This result is derived in Chapter XI of [20].

Corollary 3.3.2. *Let $J \subseteq \mathbb{R}$ be an interval whose interior is non-empty. Then*

$$\delta_{nat}(\{l \in \mathcal{P} | y_l \in J\}) > 0.$$

Proof: We assumed that there is an isomorphism $\psi : E(\mathbb{R}) \to \mathbb{R}/\mathbb{Z}$ of topological groups. Since P is a point of infinite order, $\psi(P) = \alpha + \mathbb{Z}$ must be an irrational number. Since the second projection $\pi_y : E(\mathbb{R}) \setminus \{\mathcal{O}\} \to \mathbb{R}$, $\pi_y(x,y) := y$ is onto, the set $\pi_y^{-1}(J)$ is an non-empty subset of $E(\mathbb{R})$. Furthermore, $\pi_y^{-1}(J)$ has only finitely many connected components. Since ψ is an isomorphism of topological groups, $\tilde{J} := \psi(\pi_y^{-1}(J)) \subseteq \mathbb{R}/\mathbb{Z}$ is also non-empty and has only finitely many connected components. Thus, it is the union of finitely many intervals and at least one of these intervals has non-empty interior. The assertion follows with Theorem 3.3.1 since

$$\{l \in \mathcal{P} | y_l \in J\} = \{l \in \mathcal{P} | \pi_y(l \cdot P) \in J\} = \{l \in \mathcal{P} | (l\alpha \bmod \mathbb{Z}) \in \tilde{J}\}.$$

□

With the following lemma as a last preparation we can define the set $\{l_i | i \geq 1\}$.

Lemma 3.3.3. *Let $A, B \subseteq \mathcal{P}$ with $\delta_{nat}(A) = 1$ and $\delta_{nat}(B) > 0$. Then*

$$\delta_{nat}(A \cap B) = \delta_{nat}(B).$$

Proof: Since $\delta_{nat}(\mathcal{P} \setminus A) = 0$ we have for $n \geq 1$ that

$$\frac{\#\{l \in B \setminus A | l \leq n\}}{\pi_{\mathbb{Q}}(n)} \leq \frac{\#\{l \in \mathcal{P} \setminus A | l \leq n\}}{\pi_{\mathbb{Q}}(n)} \to 0$$

as $n \to \infty$. It follows that $\delta_{nat}(B \setminus A) = 0$ and in consequence

$$\delta_{nat}(A \cap B) = \lim_{n \to \infty} \frac{\#\{l \in A \cap B | l \leq n\}}{\pi_{\mathbb{Q}}(n)}$$

$$= \lim_{n \to \infty} \left(\frac{\#\{l \in B | l \leq n\}}{\pi_{\mathbb{Q}}(n)} - \frac{\#\{l \in B \setminus A | l \leq n\}}{\pi_{\mathbb{Q}}(n)} \right) = \delta_{nat}(B) - \delta_{nat}(B \setminus A) = \delta_{nat}(B).$$

□

Theorem 3.3.4 (Existence of the sequence $(l_i)_{i\geq 1}$)**.** *There is a computable set of prime numbers* $\{l_i | i \in \mathbb{Z}_{\geq 1}\}$ *satisfying the following conditions:*

(1) $l_i \notin \mathcal{L}(P)\ \forall i \geq 1$,

(2) $l_{i+1} > l_i\ \forall i \geq 1$,

(3) $\mu_{l_i}(P) \leq 2^{-i}\ \forall i \geq 1$,

(4) $p_{l_i,l_j}(P) > 2^i\ \forall i \geq j \geq 1$ *(in particular, we require* p_{l_i,l_j} *to exist),*

(5) $p_{l_i,l}(P) > 2^i\ \forall i \geq 1\ \forall l \in \mathcal{L}(P)$ *(again, we require* $p_{l_i,l}$ *to exist),*

(6) $|y_{l_i} - i| \leq \frac{1}{10i}\ \forall i \geq 1$.

Proof: Assume that we have already found prime numbers $l_1, \ldots, l_{i-1} \in \mathcal{P}$ which satisfy the given conditions. We define for the conditions (1)-(6):

$$\mathcal{C}_j := \{l \in \mathcal{P} | l \text{ satisfies condition } (j)\}.$$

By Theorem 3.2.37 we have that $\delta_{nat}(\mathcal{C}_3) = 1$ and by Corollary 3.3.2 we have that $\delta_{nat}(\mathcal{C}_6) > 0$. With Lemma 3.3.3 it follows that $\delta_{nat}(\mathcal{C}_3 \cap \mathcal{C}_6) > 0$. Therefore, $\mathcal{C}_3 \cap \mathcal{C}_6$ is an infinite set. The sets $\mathcal{C}_1$ and $\mathcal{C}_2$ contain all sufficiently large prime numbers. By Corollary 3.2.20 this is also true for $\mathcal{C}_4$ and $\mathcal{C}_5$. Therefore, $\bigcap_{j=1}^{6} \mathcal{C}_j \neq \emptyset$ and we can define l_i as the smallest element of this set.
It remains to show that the set $\{l_i | i \geq 1\}$ is computable. We begin with verifying that, if $l_1, \ldots, l_{i-1}$ are already constructed, the sets $\mathcal{C}_i$ are computable for $1 \leq i \leq 6$. For $\mathcal{C}_1$ and $\mathcal{C}_2$ this is obviously true since $\mathcal{L}(P)$ is a finite set by Corollary 3.2.3. Since the addition on $E(\mathbb{Q})$ can be expressed through a rational function, x_n and y_n are computable functions of n by Corollary 1.3.5. Thus, $\mathcal{C}_6$ is computable. It follows from Lemma 1.2.6 and the fact that $S_0(\mathbb{Q})$ is a finite set that we can compute $S_n(P)$ as a computable function of n. Therefore, we can effectively compute $p_{l,p}(P)$ for any prime numbers l, p and the sets $\mathcal{C}_4$ and $\mathcal{C}_5$ are also computable. Since the supremum $\mu_l(P)$ is attained for some $n \leq \max S_l(P)$, $\mu_l(P)$ is a computable function of n and $\mathcal{C}_3$ is also a computable set. It follows that $\bigcap_{i=1}^{6} \mathcal{C}_i$ is a computable set and we can effectively compute the set $\{l_i | i \geq 1\}$ in ascending order. Now if we want to check if an arbitrary prime number p is an element of the set $\{l_i | i \geq 1\}$, we can compute $l_1, \ldots, l_i$ in a finite number of steps until we find a l_i such that either $l_i = p$ or $l_i > p$. □

Definition 3.3.5 (T_1 and T_2)**.** We define:

- $T_1 := \bigcup_{i\geq 1} S_{l_i}(P) \cup S_0(\mathbb{Q})$.
- $T_{2a} := \{p_l(P) | l \in \mathcal{P} \setminus \{l_i | i \geq 1\}\}$.
- $T_{2b} := \{p_{l_i,l_j}(P) | i, j \geq 1\}$.
- $T_{2c} := \{p_{l_i,l}(P) | i \geq 1, l \in \mathcal{L}(P)\}$.
- $T_2 := T_{2a} \cup T_{2b} \cup T_{2c}$.

3.4 Properties of T_1,T_2

In this section we will prove the properties of T_1 and T_2 which we have already stated in Theorem 3.1.1.

Theorem 3.4.1. $T_1 \cap T_2 = \emptyset$.

Proof: Assume that there is a $q \in T_1 \cap T_2$. Since $q \in T_1$, there is either an $i \geq 1$ such that $q \in S_{l_i}(P)$ or $q \in S_0(\mathbb{Q})$. But $q \in S_0(\mathbb{Q})$ is impossible since all elements of T_2 are elements of some set $S_n(P)$ and all these sets are disjoint with $S_0(\mathbb{Q})$. Thus, there is an $i \geq 1$ such that $q \in S_{l_i}(P)$. Now we have to consider the three cases:

- $q \in T_{2a}$. Then there is a prime number $l \neq l_i$ such that $q = p_l(P) \in S_{l^{a_l(P)}}(P) \setminus S_1(P)$. But then

  $$q \in S_{l_i}(P) \cap S_{l^{a_l(P)}}(P) = S_{(l_i,l)}(P) = S_1(P)$$

  which is a contradiction.

- $q \in T_{2b}$. Then there are $j, k \geq 1$ such that

  $$q = p_{l_j,l_k}(P) \in S_{l_j l_k}(P) \setminus (S_{l_j}(P) \cup S_{l_k}(P)).$$

  Thus, we have that $i \neq j$ and $i \neq k$. But

  $$q \in S_{l_i}(P) \cap S_{l_j l_k}(P) = S_{(l_i,l_j l_k)}(P) = S_1(P) \subseteq S_{l_j}(P)$$

  is a contradiction.

- $q \in T_{2c}$. Then there is a $j \geq 1$ and a $l \in \mathcal{L}(P)$ such that

  $$q = p_{l_j,l}(P) \in S_{l_j l}(P) \setminus (S_{l_j}(P) \cup S_l(P)).$$

  Therefore, $i \neq j$. Also, $l_i \neq l$ by construction. Then we have

  $$q \in S_{l_i}(P) \cap S_{l_j l}(P) = S_{(l_i,l_j l)}(P) = S_1(P) \subseteq S_{l_j}(P)$$

  which is a contradiction. □

Theorem 3.4.2. *T_1 is a computable set.*

Proof: First of all, we observe that $p \in T_1$ if and only if $p \in S_0(\mathbb{Q}) \cup S_1(P)$ or there is an $i \geq 1$ such that $p \in S_{l_i}(P) \setminus S_1(P)$. Since $S_0(\mathbb{Q}) \cup S_1(P)$ is a finite set, it suffices to show that there is an effective procedure to decide whether there is an $i \geq 1$ such that $p \in S_{l_i}(P) \setminus S_1(P)$. The condition $p \in S_{l_i}(P) \setminus S_1(P)$ is fulfilled if and only if $\pi_p(l_i \cdot P) = \tilde{\mathcal{O}}$ and $\pi_p(P) \neq \tilde{\mathcal{O}}$, or in other words, $\pi_p(P)$ is an element of order l_i of $E(\mathbb{F}_p)$. But the order of $\pi_p(P) \in E(\mathbb{F}_p)$ can be effectively computed and since $\{l_i | i \geq 1\}$ is a computable set by Theorem 3.3.4, this proves our assertion. □

Theorem 3.4.3. *T_2 is a computable set.*

Proof: We show that the three sets T_{2a}, T_{2b}, T_{2c} are computable.

- T_{2a}: By definition we have that $p = p_l(P) \iff p = \max(S_{l^{a_l(P)}}(P) \setminus S_1(P)) \iff p$ is the biggest prime number fulfilling $p \notin S_0(\mathbb{Q})$, $\pi_p(l^{a_l(P)} \cdot P) = \tilde{\mathcal{O}}$ and $\pi_p(P) \neq \tilde{\mathcal{O}}$. Thus, we can decide if a prime number $p \in \mathcal{P}$ is an element of T_{2a} in the following steps: 1.: Check if $p \in S_0(\mathbb{Q})$ and if $\pi_p(P) = \tilde{\mathcal{O}}$. 2.: Compute the order of $\pi_p(P) \in E(\mathbb{F}_p)$, compute $a_l(P)$ for the prime numbers l which divide the order of $\pi_p(P)$ and check if $\pi_p(l^{a_l(P)} \cdot P) = \tilde{\mathcal{O}}$. 4.: Compute $S_{l^{a_l(P)}}(P) \setminus S_1(P)$ for all l with $\pi_p(l^{a_l(P)} \cdot P) = \tilde{\mathcal{O}}$ and check if p is the biggest element of $S_{l^{a_l(P)}}(P) \setminus S_1(P)$. 5.: Check if $l \in \{l_i | i \geq 1\}$.
- T_{2b}: If $p \in T_{2b}$, then $p = p_{l_i,l_j}(P)$ with $i, j \geq 1$ and $1 \leq j \leq i < \log_2 p$ by condition (4) of Theorem 3.3.4. Thus, it suffices to compute $\max(S_{l_i l_j}(P) \setminus (S_{l_i}(P) \cup S_{l_j}(P)))$ for all $i, j \in \mathbb{N}$ with $1 \leq j \leq i < \log_2 p$.
- T_{2c}: If $p \in T_{2c}$, then $p = p_{l_i,l}(P)$ with $i \geq 1$, $l \in \mathcal{L}(P)$ and $1 \leq i < \log_2 p$ by condition (5) of Theorem 3.3.4. Thus, it suffices to compute $\max(S_{l_i l}(P) \setminus (S_{l_i}(P) \cup S_l(P)))$ for all $i \in \mathbb{N}$ with $1 \leq i < \log_2 p$ and $l \in \mathcal{L}(P)$. But since $\mathcal{L}(P)$ is a finite set, this can be done in a finite number of steps. □

Theorem 3.4.4. $\delta_{nat}(T_1) = \delta_{nat}(T_2) = 0$.

Proof: We start with T_1. Since $S_{l_i}(P) \setminus S_1(P)$ is a finite set for all $i \geq 1$, we have for all $k \geq 1$ that

$$\lim_{n\to\infty} \sum_{i=1}^{k} \frac{\#\{p \in S_{l_i}(P) \setminus S_1(P) | p \leq n\}}{\pi_{\mathbb{Q}}(n)} = 0.$$

Therefore, it is true for all $k \geq 1$ that

$$\delta^{up}_{nat}(T_1) \leq \limsup_{n\to\infty} \left(\frac{\#\{p \in S_0(\mathbb{Q}) \cup S_1(P) | p \leq n\}}{\pi_{\mathbb{Q}}(n)} + \sum_{i=1}^{\infty} \frac{\#\{p \in S_{l_i}(P) \setminus S_1(P) | p \leq n\}}{\pi_{\mathbb{Q}}(n)} \right)$$

$$\leq \sum_{i=k+1}^{\infty} \mu_{l_i}(P) \leq \sum_{i=k+1}^{\infty} 2^{-i} = 2^{-k}.$$

But this obviously implies that $\delta_{nat}(T_1) = 0$.
Since $T_{2a} \subseteq \mathcal{U}(P)$ and $\delta_{nat}(\mathcal{U}(P)) = 0$ by Theorem 3.2.35, we conclude that $\delta_{nat}(T_{2a}) = 0$.
Because of condition (4) of Theorem 3.3.4, there is a distinct pair $(i, j) \in \mathbb{N}^2$ for every $p \in T_{2b}$ with $j \leq i \leq \log_2 p$. So we have for all $n \in \mathbb{N}$ that

$$\#\{p \in T_{2b} | p \leq n\} \leq \#\{(i, j) \in \mathbb{N}^2 | 1 \leq i, j \leq \log_2 n\}.$$

Therefore, we can conclude with Theorem 3.2.34 that

$$\delta^{up}_{nat}(T_{2b}) \leq \limsup_{n\to\infty} \frac{\#\{(i, j) \in \mathbb{N}^2 | 1 \leq i, j \leq \log_2 n\}}{\pi_{\mathbb{Q}}(n)} = \limsup_{n\to\infty} \frac{O((\log n)^2)}{\frac{n}{\log n} + o(\frac{n}{\log n})} = 0.$$

In the same way it follows from condition (5) of Theorem 3.3.4 that

$$\delta^{up}_{nat}(T_{2c}) \leq \limsup_{n\to\infty} \frac{\#\mathcal{L}(P)\#\{i \in \mathbb{N} | 1 \leq i \leq \log_2 n\}}{\pi_{\mathbb{Q}}(n)} = \limsup_{n\to\infty} \frac{O(\log n)}{\frac{n}{\log n} + o(\frac{n}{\log n})} = 0.$$

□

3.5 Construction of a diophantine model of $\mathbb{Z}$

In this section we will ultimately prove Poonen's theorem. We start by describing the points on $E(\mathcal{O}_{\mathbb{Q},\mathcal{W}}) \subseteq E(\mathbb{Q})$.

Theorem 3.5.1. *Let $\mathcal{W} \subseteq \mathcal{P}$ be a set of prime numbers with $T_1 \subseteq \mathcal{W} \subseteq \mathcal{P} \setminus T_2$. Then there is a finite set $A \subseteq \mathbb{Z}$ such that for all $m \in \mathbb{Z} \setminus \{0\}$ it is true that*

$$m \cdot P \in E(\mathcal{O}_{\mathbb{Q},\mathcal{W}}) \iff m \in A \vee \exists i \geq 1 : m = \pm l_i.$$

Proof: Let $m \in \mathbb{Z} \setminus \{0\}$ such that $m \cdot P \in E(\mathcal{O}_{\mathbb{Q},\mathcal{W}})$. Then m is of the form

$$m = \pm \prod_{l \in \mathcal{P}} l^{m(l)}$$

with $m(l) = 0$ for all but finitely many $l \in \mathcal{P}$.
Now suppose that there is an $i \geq 1$ such that $m(l_i) \neq 0$. We claim that in this case $m(l_i) = 1$ and $m(l_j) = 0$ for all $j \neq i$.
Suppose that $m(l_i) > 1$. Then we have that $p_{l_i,l_i}(P) \in S_{l_i^2}(P) \subseteq S_m(P)$ by Theorem 3.2.8. Thus, $p_{l_i,l_i}(P)$ divides the denominator of y_m which implies that $p_{l_i,l_i}(P) \in \mathcal{W}$. But we also have that $p_{l_i,l_i}(P) \in T_{2b} \subseteq T_2$ which yields a contradiction to our assumption that $\mathcal{W} \cap T_2 = \emptyset$.
Now suppose that there is a $j \neq i$ such that $m(l_j) = 1$. Then it follows in the same way that $p_{l_i,l_j}(P) \in S_{l_i l_j}(P) \subseteq S_m(P)$. Consequently, we have that $p_{l_i,l_j}(P) \in \mathcal{W}$. But this is a contradiction to $p_{l_i,l_j}(P) \in T_{2b} \subseteq T_2$.
Now suppose that there is a $l \in \mathcal{P} \setminus \{l_i | i \geq 1\}$ with $m(l) \neq 0$. We claim that $m(l) \leq a_l(P) - 1$.
Suppose that $m(l) \geq a_l(P)$. Since this implies that $l^{a_l(P)}$ divides m, we can conclude that $p_l(P) \in S_{l^{a_l(P)}}(P) \subseteq S_m(P)$. Thus, $p_l(P) \in \mathcal{W}$ which is a contradiction to $p_l(P) \in T_{2a} \subseteq T_2$.
Since $a_l(P) > 1$ only for $l \in \mathcal{L}(P)$, we have that

$$m = \pm l_i^{m(l_i)} \prod_{l \in \mathcal{L}(P)} l^{m(l)}$$

with $i \geq 1$, $m(l_i) \in \{0, 1\}$ and $m(l) \leq a_l(P) - 1$ for $l \in \mathcal{L}(P)$.
We finally claim that $m(l_i) = 0$ if there is a $l \in \mathcal{L}(P)$ with $m(l) > 0$.
Suppose that there is an $i \geq 1$ and a $l \in \mathcal{L}(P)$ with $m(l_i), m(l) \geq 1$. Then we have in the same way as above that $p_{l_i,l}(P) \in \mathcal{W}$ which is a contradiction to $p_{l_i,l}(P) \in T_{2c} \subseteq T_2$.
We conclude that if $m \cdot P \in E(\mathcal{O}_{\mathbb{Q},\mathcal{W}})$, either $m = \pm l_i$ for an $i \geq 1$ or $m = \pm \prod_{l \in \mathcal{L}(P)} l^{m(l)}$ with only finitely many possibilities for the values of $m(l)$. Since $\mathcal{L}(P)$ is a finite set by Lemma 3.2.3, it only

remains to show that $\pm l_i \cdot P \in E(\mathcal{O}_{\mathbb{Q},\mathcal{W}})$ for all $i \geq 1$.
So let $i \geq 1$. Then all prime divisors of the denominator of y_{l_i} (and thus, also those of x_{l_i}) are elements of $S_{l_i}(P)$ or $S_0(\mathbb{Q})$. Since these are subsets of $T_1 \subseteq \mathcal{W}$, we conclude that $l_i \cdot P \in E(\mathcal{O}_{\mathbb{Q},\mathcal{W}})$. Since $x_{-n} = x_n$ and $y_{-n} = -y_n$ for all $n \geq 1$, it also follows that $-l_i \cdot P \in E(\mathcal{O}_{\mathbb{Q},\mathcal{W}})$ for all $i \geq 1$. □

We are now able to prove that the set $\{y_{\pm l_i} | i \geq 1\} \cup \{0\}$, which will be the diophantine model of $\mathbb{Z}$, is diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$.

Theorem 3.5.2. *Let $\mathcal{W}$ be defined as above. Then the set $\{y_{\pm l_i} | i \geq 1\}$ is diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$.*

Proof: By Theorem 3.5.1 there is a finite set $A = \{m_1, ..., m_k\} \subseteq \mathbb{Z} \setminus \{0\}$ with $A \cap \{\pm l_i | i \geq 1\} = \emptyset$ such that

$$E(\mathcal{O}_{\mathbb{Q},\mathcal{W}}) \setminus \{\mathcal{O}\} = \{\pm l_i \cdot P | i \geq 1\} \cup \{m \cdot P | m \in A\}.$$

Let $f(x, y) \in \mathbb{Z}[x, y]$ be the defining Weierstrass equation for $E(\mathbb{Q})$. Naturally, we have that $E(\mathcal{O}_{\mathbb{Q},\mathcal{W}}) \setminus \{\mathcal{O}\} = \{(x, y) \in \mathcal{O}^2_{\mathbb{Q},\mathcal{W}} | f(x, y) = 0\}$. Now we can conclude that the set

$$\{y_{\pm l_i} | i \geq 1\} = \{y \in \mathcal{O}_{\mathbb{Q},\mathcal{W}} | \exists x \in \mathcal{O}_{\mathbb{Q},\mathcal{W}} : f(x, y) = 0, (x - x_{m_1})(y - y_{m_1}) \neq 0, \ldots, (x - x_{m_n})(y - y_{m_n}) \neq 0\}$$

is diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ by Lemma 2.1.6 since $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ is dioph-regular by Theorem 2.3.5. □

Now we can finally define the following map which will yield a diophantine model of $\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$: $\Phi : \mathbb{Z} \to \mathcal{O}_{\mathbb{Q},\mathcal{W}}$,

$$\Phi(i) := \begin{cases} y_{l_i} & i \geq 1 \\ y_{-l_{-i}} & i < 0 \\ 0 & i = 0. \end{cases}$$

Now we can restate and prove Theorem 3.1.1:

Theorem 3.5.3. *Let $\mathcal{W}$ be defined as above. Then Φ defines a diophantine model of $\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$.*

Proof: First we notice that $D := \Phi(\mathbb{Z}) = \{y_{\pm l_i} | i \geq 1\} \cup \{0\}$ is diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ by Theorem 3.5.2 and Lemma 2.1.8. We also notice that $|\Phi(0) - 0| = 0$ and $|\Phi(i) - i| \leq \frac{1}{|10i|}$ for all $i \neq 0$ by our assumptions in Theorem 3.3.4 and since $y_{-n} = -y_n$ for all $n \geq 1$.
By Theorem 2.1.11 it suffices to show that the sets

$$D_+ = \{(\Phi(i), \Phi(j), \Phi(k)) | i + j = k\},$$

$$D_\times = \{(\Phi(i), \Phi(j), \Phi(k)) | ij = k\}$$

are diophantine.
To show that addition is diophantine, we claim that for all $i, j, k \in \mathbb{Z}$ it is true that

$$i + j = k \iff |\Phi(i) + \Phi(j) - \Phi(k)| < \frac{1}{3}.$$

Suppose that $i + j = k$. Then we have that

$$|\Phi(i) + \Phi(j) - \Phi(k)| = |\Phi(i) - i + \Phi(j) - j - (\Phi(k) - k)|$$

$$\leq |\Phi(i) - i| + |\Phi(j) - j| + |\Phi(k) - k| \leq \frac{1}{10} + \frac{1}{10} + \frac{1}{10} < \frac{1}{3}$$

since $|\Phi(i) - i| \leq \frac{1}{10}$ for all $i \in \mathbb{Z}$.
Conversely, suppose that some $i, j, k \in \mathbb{Z}$ fulfill $|\Phi(i) + \Phi(j) - \Phi(k)| < \frac{1}{3}$. Then we have that

$$\frac{1}{3} > |\Phi(i) - i + i + \Phi(j) - j + j - (\Phi(k) - k) - k|$$

$$\geq |i + j - k| - (|\Phi(i) - i| + |\Phi(j) - j| + |\Phi(k) - k|) > |i + j - k| - \frac{1}{3}.$$

Therefore, $|i + j - k| < \frac{2}{3}$ is fulfilled. Since $i, j, k \in \mathbb{Z}$, this is enough to conclude that $i + j = k$.
Thus, we have verified that $D_+ = \{(x, y, z) \in D^3 : |x + y - z| < \frac{1}{3}\}$. Because D^3 is diophantine by Lemma 2.1.8, we can conclude with Lemma 2.3.6 that D_+ is diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ since

$$\{x \in \mathbb{Q} : |x| < a\} = \{x \in \mathbb{Q} | \exists y_1, y_2, y_3, y_4 \in \mathbb{Q} : x^2 = y_1^2 + y_2^2 + y_3^2 + y_4^2 + a^2\}$$

for every $a \in \mathbb{Q}$, $a > 0$.
To show that multiplication is diophantine, we begin with showing that squaring is diophantine. We claim that for all $i, j \in \mathbb{Z}$ it is true that

$$i^2 = j \iff i = j = 0 \vee \left(i, j \neq 0 \wedge |\Phi(i)^2 - \Phi(j)| < \frac{2}{5}\right).$$

Suppose that $i^2 = j$ and $i, j \neq 0$. Then we have that:

$$|\Phi(i)^2 - \Phi(j)| = |\Phi(i)^2 - i^2 - (\Phi(j) - j)| \leq |\Phi(i) - i||\Phi(i) + i| + |\Phi(j) - j|$$

$$\leq \frac{1}{|10i|}\left(2|i| + \frac{1}{|10i|}\right) + \frac{1}{|10j|} < \frac{2}{10} + \frac{1}{100} + \frac{1}{10} < \frac{2}{5}$$

Conversely, suppose that $|\Phi(i)^2 - \Phi(j)| < \frac{2}{5}$ and $i, j \neq 0$. Then we have in the same way that

$$\frac{2}{5} > |\Phi(i)^2 - i^2 + i^2 - (\Phi(j) - j) - j| \geq |i^2 - j| - (|\Phi(i)^2 - i^2| + |\Phi(j) - j|) > |i^2 - j| - \frac{2}{5}.$$

Therefore, $|i^2 - j| < \frac{4}{5}$ and we can conclude that $i^2 = j$.
Now that we know that squaring is diophantine, it follows with

$$ij = k \iff (i + j)^2 = i^2 + j^2 + 2k$$

that multiplication is also diophantine.
Since Φ is obviously injective, the requirements of Theorem 2.1.11 are met. □

As a corollary of Poonen's theorem, we can show that Mazur's conjecture is wrong over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$.

Corollary 3.5.4. *There is a variety V over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ such the closure of $V(\mathcal{O}_{\mathbb{Q},\mathcal{W}})$ in $V(\mathbb{R})$ has infinitely many connected components.*

Proof: By Theorem 3.5.3, $\Phi(\mathbb{Z})$ is a discrete set which is diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$. Thus, there is an affine variety $V(\mathcal{O}_{\mathbb{Q},\mathcal{W}}) \subseteq \mathcal{O}_{\mathbb{Q},\mathcal{W}}^n$ such that $\Phi(\mathbb{Z}) = \pi_1(V(\mathcal{O}_{\mathbb{Q},\mathcal{W}}))$. But now it follows from Lemma 2.2.3 that the closure of $V(\mathcal{O}_{\mathbb{Q},\mathcal{W}})$ has infinitely many connected components. □

4 The theorem of Eisenträger and Everest

4.1 The theorem and its consequences

In this chapter we will further investigate the sets of primes $\mathcal{W}$ for which Hilbert's tenth problem is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$. It is not clear from Theorem 3.1.1 if there is a finite number of sets $\mathcal{W}_1, \ldots, \mathcal{W}_n \subseteq \mathcal{P}$ such that H10 is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{W}_i}$ for all i and these rings generate $\mathbb{Q}$ (or equivalently, $\bigcup_{i=1}^{n} \mathcal{W}_i = \mathcal{P}$). In 2009 Kirsten Eisenträger and Graham Everest proved in [3] that two such rings $\mathcal{O}_{\mathbb{Q},\mathcal{V}}$, $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ suffice to generate $\mathbb{Q}$. Moreover, the two sets $\mathcal{V}, \mathcal{W} \subseteq \mathcal{P}$ can be chosen disjoint.

Theorem 4.1.1 (Eisenträger, Everest)**.** *There are computable sets of primes $T_1, T_2, U_1, U_2 \subseteq \mathcal{P}$ with the following properties:*

- $T_1 \cap T_2 = U_1 \cap U_2 = \emptyset$.
- $T_1 \cap U_1 = T_2 \cap U_2 = \emptyset$.
- *For every set of prime numbers $\mathcal{V} \subseteq \mathcal{P}$ with $T_1 \subseteq \mathcal{V} \subseteq \mathcal{P} \setminus T_2$, the ring $\mathcal{O}_{\mathbb{Q},\mathcal{V}}$ has a diophantine model of $\mathbb{Z}$.*
- *For every set of prime numbers $\mathcal{W} \subseteq \mathcal{P}$ with $U_1 \subseteq \mathcal{W} \subseteq \mathcal{P} \setminus U_2$, the ring $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ has a diophantine model of $\mathbb{Z}$.*

Corollary 4.1.2. *There are two disjoint, computable sets of prime numbers $\mathcal{V}, \mathcal{W} \subseteq \mathcal{P}$ such that H10 is undecidable over $\mathcal{O}_{\mathbb{Q},\mathcal{V}}$ and $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$.*

Proof: Let $\mathcal{V} := T_1 \cup U_2$ and $\mathcal{W} := \mathcal{P} \setminus \mathcal{V}$. These sets are computable by Lemma 1.2.10 since $\mathcal{P}$, T_1 and U_2 are computable. Therefore, $\mathcal{O}_{\mathbb{Q},\mathcal{V}}$ and $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ are computable rings by Theorem 2.3.3. Since $\mathcal{W} = \mathcal{P} \setminus (T_1 \cup U_2)$, it follows with $T_1 \cap T_2 = U_2 \cap T_2 = \emptyset$ that $T_2 \subseteq \mathcal{W}$. In the same way it follows from $T_1 \cap U_1 = U_1 \cap U_2 = \emptyset$ that $U_1 \subseteq \mathcal{W}$. But this implies that

$$T_1 \subseteq \mathcal{V} \subseteq \mathcal{P} \setminus T_2 \text{ and } U_1 \subseteq \mathcal{W} \subseteq \mathcal{P} \setminus U_2.$$

Thus, $\mathcal{O}_{\mathbb{Q},\mathcal{V}}$ and $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ both have a diophantine model of $\mathbb{Z}$ and H10 is undecidable over these rings by Theorem 2.1.5. □

It is suggested in [3] that this result can be used to derive a kind of diophantine definition of the product group $\mathcal{O}^*_{\mathbb{Q},\mathcal{V}} \times \mathcal{O}^*_{\mathbb{Q},\mathcal{W}}$ over the group $\mathbb{Q}^*$ since every element $q \in \mathbb{Q}^*$ can be written in the form $q = st$ with $s \in \mathcal{O}^*_{\mathbb{Q},\mathcal{V}}$ and $t \in \mathcal{O}^*_{\mathbb{Q},\mathcal{W}}$ in a way that is unique up to sign. So far it is not known if this diophantine definition of groups will yield a lifiting of H10-undecidability from the rings $\mathcal{O}_{\mathbb{Q},\mathcal{V}}$ and $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ to $\mathbb{Q}$.

Our proof of Theorem 4.1.1 will have many similarities to the proof of Poonen's theorem in chapter 3. We will need a number of additional results, mainly about isogenies between elliptic curves which will be introduced in the following section.

4.2 Properties of isogenies between elliptic curves

An introduction to the theory of isogenies can be found in §4, Chapter III of [16]. Isogenies are those maps between elliptic curves which respect both their geometric and arithmetic structure as it is made clear by the following definition and theorem:

Definition 4.2.1. Let E_1 and E_2 be elliptic curves over a field K. A morphism (thus, a rational function which is regular at every point) $\phi : E_1 \to E_2$ is called *isogeny* if $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$.

Theorem 4.2.2. *Let E_1 and E_2 be elliptic curves over a field K and $\phi : E_1 \to E_2$ a non-constant isogeny. Then the following statements are true:*

- *$\phi(P +_{E_1} Q) = \phi(P) +_{E_2} \phi(Q)$ for all $P, Q \in E_1$ (here $+_{E_1}$ denotes the addition of two points on E_1 and $+_{E_2}$ the addition on E_2).*
- *$\ker(\phi)$ is a finite subgroup of E_1.*
- *There is a unique isogeny $\hat{\phi} : E_2 \to E_1$ with the property that $(\hat{\phi} \circ \phi)(P) = n \cdot P$ for all $P \in E_1$ and $(\phi \circ \hat{\phi})(Q) = n \cdot Q$ for all $Q \in E_2$ where n is the degree of ϕ. The map $\hat{\phi}$ is called the dual isogeny.*

This is proved in Theorem 4.8, Corollary 4.9 and Theorems 6.1 and 6.2, Chapter III in [16].

Remark 4.2.3. The degree of ϕ in Theorem 4.2.2 is the degree of ϕ as a map between curves, $\phi : E_1 \to E_2$. It is defined as $deg(\phi) := [K(E_1) : \phi^*(K(E_2))]$. See §2, Chapter II of [16] for related discussion.

The next theorem will serve as an analogue for Theorem 3.2.1 in this chapter. It will ensure that there are elliptic curves with certain properties from which we will construct the sets T_1, T_2, U_1 and U_2.

Theorem 4.2.4. *There are two elliptic curves E, E' defined over $\mathbb{Q}$ and an isogeny $\phi : E' \to E$ of prime degree $q \in \mathcal{P}$, $q > 2$ with the following properties:*

- *$E(\mathbb{Q}) =< P > \cong \mathbb{Z}$.*
- *E has a minimal Weierstrass equation of the form $y^2 = x^3 + B$ with $B \in \mathbb{Z}$.*
- *The generator P has integer coordinates with respect to this minimal Weierstrass equation of E.*
- *There is a rational point $P' \in E'(\mathbb{Q})$ with $\phi(P') = P$.*
- *ϕ is defined over $\mathbb{Q}$.*
- *$E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ as topological groups.*

Proof: Let E_1 be the curve defined by the equation $y^2 = x^3 - 4$ and E_2 the curve defined by $y^2 = x^3 + 108$. These curves have Conductor 432 and appear as B1 and B2 in Cremona's tables in [2]. By [2] we have that $E_1(\mathbb{Q}) \cong E_2(\mathbb{Q}) \cong \mathbb{Z}$ as well as that $E_1(\mathbb{Q})$ is generated by $P_1 = (2, 2)$ and $E_2(\mathbb{Q})$ is generated by $P_2 = (6, 18)$. According to [2] there are isogenies of degree 3 (defined over $\mathbb{Q}$) $\phi_1 : E_1 \to E_2$ and $\phi_2 : E_2 \to E_1$. The maps ϕ_1 and ϕ_2 are the dual isogenies to each other. Since ϕ_1 and ϕ_2 are group homomorphisms between $E_1(\mathbb{Q})$ and $E_2(\mathbb{Q})$, there are integers $n, m \in \mathbb{Z}$ such that $\phi_1(P_1) = n \cdot P_2$ and $\phi_2(P_2) = m \cdot P_1$. Without loss of generality, we can assume that $n, m > 0$ (if ϕ is an isogeny, then $-\phi$ is always also an isogeny). But since $(\phi_2 \circ \phi_1)(P_1) = 3 \cdot P_1$ and $(\phi_1 \circ \phi_2)(P_2) = 3 \cdot P_2$ by Theorem 4.2.2, it follows that either $n = 3$ and $m = 1$ or $n = 1$ and $m = 3$. In the first case set $E := E_1$ and $E' := E_2$, in the second case set $E := E_2$ and $E' := E_1$. The initially given Weierstrass equations for E_1 and E_2 are minimal (with respect to all primes $p \in \mathcal{P}$) by Remark 1.1, Chapter VII of [16] since $\Delta(E_1) = -2^8 3^3$ and $\Delta(E_2) = -2^8 3^9$. Also, we have that $E_1(\mathbb{R}) \cong E_2(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ since $\Delta(E_1), \Delta(E_2) < 0$ by Corollary 2.3.1, Chapter V of [18]. □

For the rest of this chapter (except where explicitly declared otherwise) we will fix two elliptic curves E, E', minimal Weierstrass equations of these curves and an isogeny $\phi : E' \to E$ of prime degree $q > 2$ with the properties of Theorem 4.2.4. Also, let $P \in E(\mathbb{Q})$ and $P' \in E'(\mathbb{Q})$ be defined as in Theorem 4.2.4.

Again, we will introduce some special notation for our handling of the elliptic curves. Notation:

- For this chapter we change the definition of $S_0(\mathbb{Q})$ to
  $S_0(\mathbb{Q}) := \{p \in \mathcal{P} : p|\Delta(E)\} \cup \{q\} = \{p \in \mathcal{P} : p|\Delta(E')\} \cup \{q\}$.
  This is well-defined by Lemma 4.2.6.
- Let x_n, y_n, $S_n(P)$, $d_n(P)$, $p_{l,p}(P)$ and π_p be defined in the same way as in chapter 3.
- Analogously to $d_n(P)$, we define $d_n(P') = \prod_{l \in \mathcal{P} \setminus S_0(\mathbb{Q})} l^{\max\{-\operatorname{ord}_l(x(n \cdot P')), 0\}}$.
- For $n \neq 0$ let $D_n(P) := \{p \in \mathcal{P} | \operatorname{ord}_p(x_n) < 0\}$.
  (Notice that $D_1(P) = S_1(P) = \emptyset$ since P has integral coordinates.)
- For $l \in \mathcal{P}$ let $b_l(P) := \min\{n \geq 1 | \# S_{l^n}(P) \geq 2\}$.
  (This is well-defined by Corollary 4.2.21.)
- Let $\mathcal{L}(P) := \{l \in \mathcal{P} | b_l(P) > 1\}$.
- Let $p_l(P) := \max S_{l^{b_l(P)}}$ and $p'_l(P) := \max(S_{l^{b_l(P)}} \setminus \{p_l(P)\})$.
- Let $d_n^*(P)$ denote the largest positive integer with $d_n^*(P) \mid d_n(P)$ and $(d_n^*(P), d_m(P)) = 1$ for all $m < n$. Define $d_n^*(P')$ analogously.
- Define sequences $(A_n)_{n \geq 1}$, $(B_n)_{n \geq 1}$ and $(C_n)_{n \geq 1}$ through

$$n \cdot P = \left(\frac{A_n}{B_n^2}, \frac{C_n}{B_n^3} \right)$$

  where $A_n, B_n, C_n \in \mathbb{Z}$, $B_n > 0$ and $(A_n C_n, B_n) = 1$ for all $n \geq 1$.

The sets $D_n(P)$ have the same important property as the sets $S_n(P)$:

Theorem 4.2.5. *$D_m(P) \cap D_n(P) = D_{(m,n)}(P)$ for all $m, n \in \mathbb{Z} \setminus \{0\}$.*

This can be proved in exactly the same way as Theorem 3.2.8. The next lemma ensures that $S_0(\mathbb{Q})$ is well-defined.

Lemma 4.2.6. *E and E' share the same set of bad reduction primes (thus, primes p for which the reduced curve $E(\mathbb{F}_p)$ for the minimal Weierstrass equation is singular).*

This is an immediate consequence of Corollary 7.2, Chapter VII of [16], p. 185.
The rest of this chapter will be dedicated to proving that $\mathcal{L}(P)$ is a finite set, or in other words, $d_l(P)$ has two different prime divisors for all but finitely many $l \in \mathcal{P}$. We begin with introducing a theorem of Joseph Silverman for which we will need the following definition:

Definition 4.2.7. A prime number $p \in \mathcal{P}$ is called a primitive prime divisor of B_n if $p \mid B_n$ and $(p, B_m) = 1$ for all $m \in \{1, \ldots, n-1\}$.

Theorem 4.2.8 (Silverman)**.** *Let E be an elliptic curve over $\mathbb{Q}$ in Weierstrass form and $P \in E(\mathbb{Q})$ a point of infinite order. Let the sequence $(B_n)_{n\geq 1}$ be defined as above. Then there is a $N_0 \in \mathbb{N}$ such that B_n has at least one primitive prime divisor for all $n \geq N_0$.*

This is Proposition 10 of [17], p. 234.

Corollary 4.2.9. *There is a $N_1 \in \mathbb{N}$ such that $d_n^*(P') > 1$ for all $n \geq N_1$.*

Proof: This is obvious from Theorem 4.2.8 since $S_0(\mathbb{Q})$ is a finite set. □

We want to use this last result to show that $d_l(P)$ has at least two different prime divisors for all but finitely many $l \in \mathcal{P}$. We will employ the isogeny ϕ to establish a relation between $d_l(P')$ and $d_l(P)$.
We begin with introducing a more general notation of the canonical height which will allow us to establish a relation between the canonical heights of P' and $P = \phi(P')$ and the degree of ϕ:

Theorem 4.2.10 (Tate)**.** *Let E be an elliptic curve over $\mathbb{Q}$, $P \in E(\mathbb{Q})$ and $f \in \mathbb{Q}(E)$ a non-constant even function (thus, a rational morphism $f : E \subseteq \mathbb{P}(\mathbb{Q})^2 \to \mathbb{P}(\mathbb{Q})$ fulfilling $f(Q) = f(-Q)$ for all $Q \in E(\mathbb{Q})$). Then*

$$\frac{1}{\deg(f)} \lim_{n\to\infty} 4^{-n} h(f(2^n \cdot P)) = \hat{h}(P).$$

($\deg(f)$ is the degree of f as a map between curves, see Remark 4.2.3.)

This is Proposition 9.1, Chapter VIII of [16], p. 228. (Silverman actually uses this as a definition of canonical height in [16]. This obviously extends our notion of canonical height since the map f_x in Definition 3.2.13 fulfills $f_x(Q) = f_x(-Q)$ for all points $Q \in E(\mathbb{Q})$ and $\deg(f_x) = 2$.)

Lemma 4.2.11. *$\hat{h}(P) = q\hat{h}(P')$.*

Proof: Beforehand, recall the definition of f_x from Definition 3.2.13 and notice that $f_x \circ \phi$ is an even function on E'. Then it follows that

$$\hat{h}(P) = \hat{h}(\phi(P')) = \frac{1}{2} \lim_{n\to\infty} 4^{-n} h(f_x(2^n \cdot \phi(P')))$$

$$= \frac{1}{2} \lim_{n\to\infty} 4^{-n} h(f_x(\phi(2^n \cdot P'))) = \frac{q}{deg(f_x \circ \phi)} \lim_{n\to\infty} 4^{-n} h((f_x \circ \phi)(2^n \cdot P')) = q\hat{h}(P').$$

□

We already derived the estimation $\log d_n(P) = \hat{h}(P)n^2 + o(n^2)$ in the Lemmata 3.2.14 and 3.2.18. In this chapter we will need a somewhat stronger estimate which we will carry over from [5].

Theorem 4.2.12. *Let E be an elliptic curve defined over $\mathbb{Q}$ in Weierstrass form, P a point of infinite order on $E(\mathbb{Q})$ and let the sequence $(B_n)_{n\geq 1}$ be defined as above. Further, let $S \subseteq \mathcal{P}$ be a finite set of primes and define $|x|_S := \prod_{p\notin S} p^{\mathrm{ord}_p(x)}$ for $x \in \mathbb{Z}\setminus\{0\}$. Then there is a constant $K > 0$ such that*

$$\log |B_n|_S = \hat{h}(P)n^2 + O((\log n)^K)$$

as $n \to \infty$.

This is Lemma 2.2 of [5].

Corollary 4.2.13. *There is a $K > 0$ such that*

$$\log d_n(P) = 2\hat{h}(P)n^2 + O((\log n)^K),$$

$$\log d_n(P') = \frac{2}{q}\hat{h}(P)n^2 + O((\log n)^K).$$

Proof: This follows from Lemma 4.2.11 and Theorem 4.2.12 since $S_0(\mathbb{Q})$ is a finite set and $d_n(P) = |B_n^2|_{S_0(\mathbb{Q})}$. □

We will also use the following rough estimate for the sum of all squares of prime numbers:

Lemma 4.2.14.

$$\sum_{p\in\mathcal{P}} \frac{1}{p^2} < \frac{1}{2}.$$

Proof: By a well-known result we have that $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$. Therefore, we can conclude that

$$\sum_{p\in\mathcal{P}} \frac{1}{p^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} - \sum_{n\in\mathbb{N}_{\geq 1}\setminus\mathcal{P}} \frac{1}{n^2}$$

$$< \frac{\pi^2}{6} - \left(1 + \frac{1}{4^2} + \frac{1}{6^2} + \frac{1}{8^2} + \frac{1}{9^2} + \frac{1}{10^2} + \frac{1}{12^2} + \frac{1}{14^2} + \frac{1}{15^2} + \frac{1}{16^2}\right) = \frac{\pi^2}{6} - \frac{29177437}{25401600} < \frac{1}{2}.$$

□

These results allow us to prove the following technical lemma:

Lemma 4.2.15. *There is a $N_2 \in \mathbb{N}$ such that $d_n(P') \neq d_n^*(P)$ for all $n > N_2$.*

Proof: We begin with claiming for all $n \geq 1$ that

$$d_n(P) \mid d_n^*(P) \prod_{p\in\mathcal{P}, p\mid n} p^2 d_{\frac{n}{p}}(P). \tag{4.2.1}$$

Indeed, let $l \in \mathcal{P}$ be a prime with $l \mid d_n(P)$ and $l \nmid d_n^*(P)$. Thus, there is a $m < n$ such that $l \mid d_m(P)$. Corollary 3.2.12 implies that there is a $p \in \mathcal{P}$ with $p \mid n$ and $l \mid d_{\frac{n}{p}}(P)$. It also follows with Corollary 3.2.12 that

$$\operatorname{ord}_l(d_n(P)) = \operatorname{ord}_l(d_{\frac{n}{p}}(P)) + 2\operatorname{ord}_l(p).$$

But this already implies the equation (4.2.1). It follows that

$$\log d_n^*(P) \geq \log d_n(P) - \sum_{p|n} \log p^2 - \sum_{p|n} \log d_{\frac{n}{p}}(P).$$

By Corollary 4.2.13 there is a $K > 0$ such that

$$\log d_n(P) = 2\hat{h}(P)n^2 + O((\log n)^K) = 2\hat{h}(P)n^2 + o(n^2).$$

We also have that

$$\sum_{p|n} \log p^2 = \log \prod_{p|n} p^2 \leq \log n^2 = o(n^2),$$

$$\sum_{p|n} \log d_{\frac{n}{p}}(P) = \sum_{p|n} \left(2\hat{h}(P)\frac{n^2}{p^2} + O((\log n)^K) \right) = 2\hat{h}(P)n^2 \sum_{p|n} \frac{1}{p^2} + O(\pi_{\mathbb{Q}}(n) \cdot (\log n)^K).$$

It follows from Theorem 3.2.34 that $O(\pi_{\mathbb{Q}}(n) \cdot (\log n)^K) = o(n^2)$.
Since $\sum_{p \in \mathcal{P}} \frac{1}{p^2} < \frac{1}{2}$ by Lemma 4.2.14, we have now derived that

$$\log d_n^*(P) > \hat{h}(P)n^2 + o(n^2). \tag{4.2.2}$$

We also have

$$\log d_n(P') = \frac{2}{l}\hat{h}(P)n^2 + o(n^2). \tag{4.2.3}$$

by Corollary 4.2.13.
Now suppose that $d_n^*(P) = d_n(P')$. Then it follows from (4.2.2) and (4.2.3) that

$$\hat{h}(P)n^2 < \frac{2}{l}\hat{h}(P)n^2 + o(n^2).$$

But we can choose n large enough to rule this case out since $l > 2$ and $\hat{h}(P) \neq 0$. □

To establish a relation between $d_n(P)$ and $d_n(P')$, we will introduce certain formulae for isogenies over $\mathbb{Q}$. To make sure that these formulae apply to our isogeny ϕ, we will make use of the following theorem, which tells us that an isogeny is essentially determined by its kernel.

Theorem 4.2.16. *Let E be an elliptic curve over an algebraically closed field K and let $F \subseteq E(K)$ be a finite subgroup of $E(K)$. Then there is a unique elliptic curve E' over K and a unique separable isogeny $\psi : E(K) \to E'(K)$ such that $\ker(\psi) = F$. The curve E' is denoted as E/F.*

This is Proposition 4.12, Chapter III of [16], p. 78 (the uniqueness of the isogeny ψ follows with Corollary 4.11, Chapter III of [16]).
It applies to our isogeny ϕ since all non-constant isogenies over $\overline{\mathbb{Q}}$ are separable.

Formulae for E/F:

Let E be an arbitrary elliptic curve over an algebraically closed field and F a finite subgroup. Jaques Vélu's article [19] provides us with formulae for the isogeny $\psi : E \to E/F$ which we will use later on to establish a relationship between $\mathrm{ord}_p(d_n(P))$ and $\mathrm{ord}_p(d_n(P'))$. Our techniques are very similar to those used in [5].

Vélu's formulae take E to be in Weierstrass form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We define

$$b_2 := a_1^2 + 4a_2, \quad b_4 := a_1a_3 + 2a_4, \quad b_6 := a_3^2 + 4a_6.$$

To make things less complicated, we assume that $\#F = q \in \mathcal{P}$ and $q > 2$. Let Q denote a generator of F and let $\hat{x}_k := x(k \cdot Q)$ for $1 \leq k < q$. We further define:

$$t_k := 6\hat{x}_k^2 + b_2\hat{x}_k + b_4,$$

$$u_k := 4\hat{x}_k^3 + b_2\hat{x}_k^2 + 2b_4\hat{x}_k + b_6,$$

$$w_k := u_k + \hat{x}_k t_k,$$

$$t := \sum_{k=1}^{(q-1)/2} t_k, \quad u := \sum_{k=1}^{(q-1)/2} u_k, \quad w := \sum_{k=1}^{(q-1)/2} w_k.$$

Then E/F has a Weierstrass equation of the form

$$y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6' \tag{4.2.4}$$

where

$$a_1' := a_1, \quad a_2' := a_2, \quad a_3' := a_3, \quad a_4' := a_4 - 5t, \quad a_6' := a_6 - b_2t - 7w.$$

Further, let $P = (x, y) \notin F$ denote a point of infinite order on E in Weierstrass coordinates. Then we have that

$$x(\psi(P)) = x + \sum_{k=1}^{(q-1)/2} \left(\frac{t_k}{x - \hat{x}_k} + \frac{u_k}{(x - \hat{x}_k)^2} \right). \tag{4.2.5}$$

with respect to the established Weierstrass equation of E/F. If the curve E is defined over $\mathbb{Q}$, it is possible that $Q \notin E(\mathbb{Q})$, but the formulae will still produce a Weierstrass equation over $\mathbb{Q}$ for E/F and a rational image $\psi(P) \in (E/F)(\mathbb{Q})$ for every rational point $P \in E(\mathbb{Q})$.

The above formulae may not produce a minimal Weierstrass equation for E/F, so we will need the following theorem:

Theorem 4.2.17. *Let $p \in \mathcal{P}$ be a prime number and let E be an elliptic curve over $\mathbb{Q}_p$ with Weierstrass coordinates (x, y). Then any change of coordinates $(x, y) \mapsto (x', y')$ such that E has a minimal Weierstrass equation with respect to p and the coordinates (x', y') is of the form*

$$x = u^2 x' + r, \tag{4.2.6}$$

$$y = u^3 y' + u^2 s x' + t$$

where $u, r, s, t \in \mathbb{Z}_p$.

This is Proposition 1.3 (d), Chapter VII of [16], p. 172-173.
We also need the following technical lemma which gives us a handy description of the set of points of order $p > 2$ on E:

Lemma 4.2.18. *Let E be an elliptic curve over $\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{Z}$. Let $p \in \mathcal{P}$, $p > 2$. Then there is a polynomial $\psi_p \in \mathbb{Z}[x]$ of degree $(p^2 - 1)/2$ with leading coefficient p such that*

$$E(\overline{\mathbb{Q}})[p] \setminus \{\mathcal{O}\} = \{Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\} | \psi_p(x(Q)) = 0\}.$$

This is contained in Exercise 3.7, Chapter III of [16], p. 105.
Now we can finally show how $d_n(P)$ and $d_n(P')$ are connected:

Lemma 4.2.19. $\operatorname{ord}_p(d_n(P')) \leq \operatorname{ord}_p(d_n(P)) \leq \operatorname{ord}_p(d_{qn}(P'))$ *for all $p \in \mathcal{P}$ and $n \geq 1$.*

Proof: Let $n \geq 1$ and let $p \in \mathcal{P}$ such that $p \mid d_n(P')$. Since ϕ is a separable isogeny, we know from Theorem 4.2.16 that $E'/\ker(\phi)$ and E are the same curve (observe that $\ker(\phi)$ is a finite subgroup of E' by Theorem 4.2.2 since ϕ is not constant). Since we do not know if the Weierstrass equation for $E'/\ker(\phi)$ provided by (4.2.4) is minimal with respect to p we can only say that $\phi = f \circ \psi$ where ψ is the isogeny described through Vélu's formula (4.2.5) and f is a change of coordinates of the form (4.2.6).
At first we will show that $\operatorname{ord}_p(x(n \cdot P')) = \operatorname{ord}_p(x(\psi(n \cdot P')))$. Let

$$n \cdot P' = \left(\frac{X}{Y^2}, \frac{Z}{Y^3}\right)$$

where $X, Y, Z \in \mathbb{Z}$, $Y \geq 1$ and $(XZ, Y) = 1$. Then (4.2.5) implies that

$$x(\psi(n \cdot P')) = \frac{X}{Y^2} + \sum_{k=1}^{(q^2-1)/2} \left(\frac{t_k Y^2}{X - \hat{x}_k Y^2} + \frac{u_k Y^4}{(X - \hat{x}_k Y^2)^2}\right).$$

As mentioned above, it is possible that $\hat{x}_k \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$. In this case, we have to consider the extension $\mathbb{Q}(\hat{x}_1, \ldots, \hat{x}_{q-1})$.
In case that all $\hat{x}_k$ are algebraic integers (and therefore, also all t_k and u_k), we have that $\operatorname{ord}_p(X - \hat{x}_k Y^2) = 0$ since $(X, Y) = 1$ and $\operatorname{ord}_p(Y) > 0$ by assumption. Then it follows that

either

$$\operatorname{ord}_p\left(\sum_{k=1}^{(q-1)/2}\left(\frac{t_kY^2}{X-\hat{x}_kY^2}+\frac{u_kY^4}{(X-\hat{x}_kY^2)^2}\right)\right)>0$$

or the sum is equal to 0. This implies

$$\operatorname{ord}_p(x(\psi(n\cdot P')))=\operatorname{ord}_p\left(\frac{X}{Y^2}+\sum_{k=1}^{(q-1)/2}\left(\frac{t_kY^2}{X-\hat{x}_kY^2}+\frac{u_kY^4}{(X-\hat{x}_kY^2)^2}\right)\right)$$

$$=-2\operatorname{ord}_p(Y)=\operatorname{ord}_p(x(n\cdot P')).$$

Now suppose that not all $\hat{x}_k$ are integers. By Lemma 4.2.18 the equation for the x-coordinates of points of order q on $E'(\overline{\mathbb{Q}})$ is a polynomial with integer coefficients of order $(q^2-1)/2$ with leading coefficient q. Therefore, all $q\hat{x}_k$ are integers. Now we employ a change of coordinates on E', $g(x,y):=(q^2x,q^3y)$, which changes the Weierstrass equation of E' into

$$y^2=x^3+a_4q^4x+a_6q^6.$$

Notice that we do not lose generality through this change of coordinates since $\operatorname{ord}_p(q^2x)=\operatorname{ord}_p(x)$ ($p\neq q$ since $q\in S_0(\mathbb{Q})$). But if we now use Vélu's formula for the new Weierstrass-coordinates of E', the x-coordinates of the non-zero points in $\ker(\psi)$, $\hat{x}'_k=q^2\hat{x}_k$ are integers and the proof of the first case applies.
In the next step we will show that $\operatorname{ord}_p(x(f(\psi(n\cdot P'))))\leq\operatorname{ord}_p(x(\psi(n\cdot P')))$. But this follows immediately from Theorem 4.2.17: Let $\bar{x}:=x(\psi(n\cdot P'))$. Then we have that

$$\operatorname{ord}_p(\bar{x})=\operatorname{ord}_p(x(\psi(n\cdot P')))=\operatorname{ord}_p(x(n\cdot P'))<0$$

(since $p\mid d_n(P')$) and there are $\bar{u},\bar{r}\in\mathbb{Z}_p$ such that

$$\operatorname{ord}_p(x(f(\psi(n\cdot P'))))=\operatorname{ord}_p\left(\frac{\bar{x}-\bar{r}}{\bar{u}^2}\right)=\operatorname{ord}_p(\bar{x})-2\operatorname{ord}_p(\bar{u})\leq\operatorname{ord}_p(\bar{x})=\operatorname{ord}_p(x(\psi(n\cdot P'))).$$

Altogether, we have shown that $\operatorname{ord}_p(x(n\cdot P'))\geq\operatorname{ord}_p(x(\phi(n\cdot P')))$ and if we apply the same technique to the dual isogeny $\hat{\phi}:E\to E'$, it follows that

$$\operatorname{ord}_p(x(n\cdot P'))\geq\operatorname{ord}_p(x(\phi(n\cdot P')))=\operatorname{ord}_p(x(n\cdot P))\geq\operatorname{ord}_p(x(\hat{\phi}(n\cdot P)))=\operatorname{ord}_p(x(qn\cdot P')).$$

This concludes our proof. □

Now we have all the requirements to show that $d_n(P)$ has two distinct prime divisors for almost all n (which will have as a consequence that $\mathcal{L}(P)$ is a finite set).

Theorem 4.2.20. *There is a $N_3\in\mathbb{N}$ such that there are $p_n,q_n\in\mathcal{P}$, $p_n\neq q_n$ with $p_nq_n\mid d_n^*(P)$ for all $n\geq N_3$ with $(n,q)=1$.*

Proof: Let N_1 be defined as in Corollary 4.2.9 and N_2 as in Lemma 4.2.15. Let $n\geq\max\{N_1,N_2\}$. Then there is a $p_n\in\mathcal{P}$ with $p_n\mid d_n^*(P')$.
We claim that $p_n\mid d_n^*(P)$. It follows from Lemma 4.2.19 that $p_n\mid d_n(P)$. Now suppose that there is a $m<n$ with $p_n\mid d_m(P)$ and let m be minimal with this property. This implies that $\operatorname{ord}(\pi_{p_n}(P))=m$

in $E(\mathbb{F}_{p_n})$. But since $n \cdot \pi_{p_n}(P) = \pi_{p_n}(n \cdot P) = \tilde{\mathcal{O}}$, it follows that $m \mid n$. It also follows in the same way from Lemma 4.2.19 that $p_n \mid d_{qm}(P')$ and $qm \cdot \pi_{p_n}(P') = \tilde{\mathcal{O}}$. But since $\mathrm{ord}(\pi_{p_n}(P')) = n$ in $E'(\mathbb{F}_{p_n})$, this implies $n \mid qm$. Since $n \neq m$, this would imply that $n = qm$ which is a contradiction to $(n, q) = 1$. Therefore, $p_n \mid d_n^*(P)$.
Now we claim that there is a $q_n \in \mathcal{P}$ with $q_n \mid d_n^*(P)$ and $q_n \nmid d_n(P')$ (this obviously implies $p_n \neq q_n$). Suppose we have for all $q_n \in \mathcal{P}$ with $q_n \mid d_n^*(P)$ that $q_n \mid d_n(P')$. Then it follows from Lemma 4.2.15 that there is a $q_n \in \mathcal{P}$ with $0 < \mathrm{ord}_{q_n}(d_n(P')) < \mathrm{ord}_{q_n}(d_n(P))$. But now it follows from Lemma 4.2.19 and Corollary 3.2.12 that

$$\mathrm{ord}_{q_n}(d_n(P')) < \mathrm{ord}_{q_n}(d_n(P)) \leq \mathrm{ord}_{q_n}(d_{qn}(P')) = \mathrm{ord}_{q_n}(d_n(P')) + 2\,\mathrm{ord}_{q_n}(q).$$

But this would imply that $q = q_n$ which is a contradiction since $q \in S_0(\mathbb{Q})$. □

Corollary 4.2.21. (1) *For every $l \in \mathcal{P}$ the value $b_l(P)$ is well-defined.*

(2) *There are only finitely many $l \in \mathcal{P}$ with $b_l(P) > 1$ (thus, $\mathcal{L}(P)$ is a finite set).*

Proof: Let $l \in \mathcal{P}$. The quantity $b_l(P)$ is well-defined by Theorem 3.2.2. Now let N_3 be defined as in Theorem 4.2.20. Then we have for all prime numbers $l \in \mathcal{P}$ with $l \geq N_3$ and $l \neq q$ that $\#S_l(P) \geq 2$ and $b_l(P) = 1$. □

4.3 Construction of T_1, T_2, U_1 and U_2

The rest of this chapter is very similar to the corresponding parts in chapter 3. Therefore, we will only refer to the proofs in chapter 3 for most of the results.

Theorem 4.3.1. *There are two computable sets of prime numbers $\{l_i | i \geq 1\}$ and $\{l_i' | i \geq 1\}$ satisfying the following conditions:*

(1) $\{l_i | i \geq 1\} \cap \{l_i' | i \geq 1\} = \emptyset$,

(2) $l_i, l_i' \notin \mathcal{L}(P)$ $\forall i \geq 1$,

(3) $l_{i+1} > l_i$ *and* $l_{i+1}' > l_i'$ $\forall i \geq 1$,

(4) $p_{l_i, l_j}(P) > 2^i$ *and* $p_{l_i', l_j'}(P) > 2^i$ $\forall i \geq j \geq 1$,

(5) $p_{l_i, l}(P) > 2^i$ *and* $p_{l_i', l}(P) > 2^i$ $\forall i \geq 1$ $\forall l \in \mathcal{L}(P)$,

(6) $|y_{l_i} - i| \leq \frac{1}{10i}$ *and* $|y_{l_i'} - i| \leq \frac{1}{10i}$ $\forall i \geq 1$.

Proof: Naturally, the proof is very similar to the proof of Theorem 3.3.4.
Let $i \geq 1$ and assume that we have already found prime numbers $l_1, \ldots, l_{i-1}$ and $l_1', \ldots, l_{i-1}'$ which satisfy the given conditions. Since the set $\{l \in \mathcal{P} : |y_l - i| \leq \frac{1}{10i}\}$ has positive natural density by Corollary 3.3.2, it contains infinitely many prime numbers. By Corollary 3.2.20 and since $\mathcal{L}(P)$ is a finite set, condition (4) and (5) are fulfilled for all sufficiently large numbers. Therefore, we can find $l_i, l_i' \in \mathcal{P}$, $l_i \neq l_i'$ which satisfy the given conditions.
The sets are computable due to the same arguments used in the proof of Theorem 3.3.4. □

Definition 4.3.2 (T_1, T_2, U_1, U_2)**.** We define:

- $T_1 := \bigcup_{i\geq 1} D_{l_i}(P)$.
- $U_1 := \bigcup_{i\geq 1} D_{l'_i}(P)$.
- $T_{2a} := \{p_l(P) | l \in \mathcal{P} \setminus \{l_i | i \geq 1\}\}$.
- $T_{2b} := \{p_{l_i,l_j}(P) | i, j \geq 1\}$.
- $T_{2c} := \{p_{l_i,l}(P) | i \geq 1, l \in \mathcal{L}(P)\}$.
- $T_2 := T_{2a} \cup T_{2b} \cup T_{2c}$.
- $U_{2a} := \{p'_l(P) | l \in \mathcal{P} \setminus \{l'_i | i \geq 1\}\}$.
- $U_{2b} := \{p_{l'_i,l'_j}(P) | i, j \geq 1\}$.
- $U_{2c} := \{p_{l'_i,l}(P) | i \geq 1, l \in \mathcal{L}(P)\}$.
- $U_2 := U_{2a} \cup U_{2b} \cup U_{2c}$.

4.4 Properties of T_1, T_2, U_1, U_2

Theorem 4.4.1. $T_1 \cap U_1 = T_2 \cap U_2 = T_1 \cap T_2 = U_1 \cap U_2 = \emptyset$.

Proof: $T_1 \cap T_2 = U_1 \cap U_2 = \emptyset$ can be proved in exactly the same fashion as Theorem 3.4.1.
$T_1 \cap U_1 = \emptyset$ follows from the fact that $l_i \neq l'_j$ for all $i, j \geq 1$ which implies $D_{l_i}(P) \cap D_{l'_j}(P) = D_1(P) = \emptyset$ by Theorem 4.2.5.
Now suppose that there is a $p \in T_2 \cap U_2$. We have to consider three cases:

- If $p \in T_{2a}$, there is a $l \in \mathcal{P}$ such that $p = p_l(P)$. Suppose that $p_l(P) \in U_{2a}$. Then there is a $l' \in \mathcal{P}$ such that $p = p'_{l'}(P)$. But now it follows from Theorem 3.2.8 that $l = l'$ and this would imply that $p_l(P) = p'_l(P)$ which is a contradiction.
  If $p_l(P) \in U_{2b}$, there are $i, j \geq 1$ such that

  $$p_l(P) = p_{l'_i,l'_j}(P) \in S_{l'_i l'_j}(P) \setminus (S_{l'_i}(P) \cup S_{l'_j}(P)).$$

  But $p_l(P) \in S_{l'_i l'_j}(P)$ would imply that $l = l'_i$ or $l = l'_j$ and this is a contradiction to the fact $p_l(P) \notin S_{l'_i}(P) \cup S_{l'_j}(P)$.
  Due to the same reason $p_l(P) \in U_{2c}$ can be ruled out.

- If $p \in T_{2b}$, there are $i, j \geq 1$ such that $p = p_{l_i,l_j}(P)$. Due to the reasons explained above $p \in U_{2a}$ is impossible.
  It is impossible that $p_{l_i,l_j}(P) \in U_{2b}$ since $S_{l_i,l_j}(P) \cap S_{l'_m,l'_n}(P) = \emptyset$ for all $m, n \geq 1$ due to $\{l_i | i \geq 1\} \cap \{l'_i | i \geq 1\} = \emptyset$.
  If $p_{l_i,l_j}(P) \in U_{2c}$, there is a $m \geq 1$ and a $l \in \mathcal{L}(P)$ such that $p_{l_i,l_j}(P) = p_{l'_m,l}(P)$. But this is also impossible because $l_i, l_j \neq l'_i$ and $l_i, l_j \neq l$ since $\mathcal{L}(P) \cap \{l_i | i \geq 1\} = \emptyset$.

- If $p \in T_{2c}$, there is a $i \geq 1$ and a $l \in \mathcal{L}(P)$ such that $p = p_{l_i,l}(P)$. Both $p \in U_{2a}$ and $p \in U_{2b}$ can be ruled out due to the same reasons explained above. If $p_{l_i,l}(P) \in U_{2c}$, there is a $j \geq 1$ and a $l' \in \mathcal{L}(P)$ such that $p_{l_i,l}(P) = p_{l'_j,l'}(P)$. This implies that $l = l'$. But since $l_i \neq l'_j$ for all $j \geq 1$, we have that $p \in S_{l_i l}(P) \cap S_{l'_j l}(P) = S_l(P)$. But this is impossible since $p_{l_i,l} \notin S_l(P)$. □

Theorem 4.4.2. *T_1, T_2, U_1 and U_2 are all computable sets.*

Proof: Since $T_1 \setminus S_0(\mathbb{Q}) = \bigcup_{i \geq 1} S_{l_i}(P)$, $T_1 \cap S_0(\mathbb{Q})$ is a finite set and $\{l_i | i \geq 1\}$ is a computable set, the computability of T_1 can be proved in the same fashion as in Theorem 3.4.2. The set U_1 is computable due to a similar reason since $\{l'_i | i \geq 1\}$ is computable. The computability of T_2 and U_2 can be proved in the same way as Theorem 3.4.3. □

4.5 Construction of a diophantine model of $\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q},\mathcal{V}}$ and $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$

Theorem 4.5.1. *Let $\mathcal{V} \subseteq \mathcal{P}$ be a set of prime numbers with $T_1 \subseteq \mathcal{V} \subseteq \mathcal{P} \setminus T_2$. Then $\mathcal{O}_{\mathbb{Q},\mathcal{V}}$ has a diophantine model of $\mathbb{Z}$.*

Proof: It can be proved in exactly the same fashion as in Theorem 3.5.1 that there is a finite set $A \subseteq \mathbb{Z}$ such that

$$m \cdot P \in E(\mathcal{O}_{\mathbb{Q},\mathcal{V}}) \iff m \in A \vee \exists i \geq 1 : m = \pm l_i$$

for all $m \in \mathbb{Z} \setminus \{0\}$.
Then it follows analogously to Theorem 3.5.2 that $\{y_{\pm l_i} | i \geq 1\}$ is diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{V}}$.
But then the map $\Phi_{\mathcal{V}} : \mathbb{Z} \to \mathcal{O}_{\mathbb{Q},\mathcal{V}}$,

$$\Phi_{\mathcal{V}}(i) := \begin{cases} y_{l_i} & i \geq 1 \\ y_{-l_{-i}} & i < 0 \\ 0 & i = 0 \end{cases}$$

yields a diophantine model of $\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q},\mathcal{V}}$. The proof is exactly the same we had for Theorem 3.5.3. □

Theorem 4.5.2. *Let $\mathcal{W} \subseteq \mathcal{P}$ be a set of prime numbers with $U_1 \subseteq \mathcal{W} \subseteq \mathcal{P} \setminus U_2$. Then $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ has a diophantine model of $\mathbb{Z}$.*

Proof: Unsurprisingly, the proof is very similar to the proof of Theorem 4.5.1. There is a finite set $B \subseteq \mathbb{Z}$ such that

$$m \cdot P \in E(\mathcal{O}_{\mathbb{Q},\mathcal{W}}) \iff m \in B \vee \exists i \geq 1 : m = \pm l'_i$$

for all $m \in \mathbb{Z} \setminus \{0\}$. The set $\{y_{\pm l'_i} | i \geq 1\}$ is diophantine over $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$ and the map $\Phi_{\mathcal{W}} : \mathbb{Z} \to \mathcal{O}_{\mathbb{Q},\mathcal{W}}$,

$$\Phi_{\mathcal{W}}(i) := \begin{cases} y_{l'_i} & i \geq 1 \\ y_{-l'_{-i}} & i < 0 \\ 0 & i = 0 \end{cases}$$

yields a diophantine model of $\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q},\mathcal{W}}$. □

Bibliography

[1] G. Cornelissen, K. Zahidi, Topology of diophantine sets: Remarks on Mazur's conjectures, in: J. Denef et al. (eds.), *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, *Contemp. Math.* **270**, AMS, Providence, RI, 2000, pp. 253-260.

[2] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, second edition, Cambridge University Press, Cambridge, 1997.

[3] K. Eisenträger, G. Everest, Descent on elliptic curves and Hilbert's tenth problem, *Proc. Amer. Math. Soc.* **137** (2009), 1951-1959.

[4] M. D. Fried, M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, 1986.

[5] G. Everest, V. Miller, N. Stephens, Primes generated by elliptic curves, *Proc. Amer. Math. Soc.* **132** (2004), 955-963.

[6] S. Lang, *Algebraic Number Theory*, Springer-Verlag, New York, 1994.

[7] Yu. V. Matiyasevich, *Hilbert's Tenth Problem*, MIT Press, Cambridge, MA, 1993.

[8] B. Mazur, The topology of rational points, *Experiment. Math.* **1** (1992), 35-45.

[9] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, third ed., Springer-Verlag, Berlin, 2004.

[10] B. Poonen, Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$, *J. Amer. Math. Soc.* **16** (2003), 981-990.

[11] H. Rogers, *Theory of Recursive Functions and Effective Computability*, McGraw-Hill, New York-Toronto, Ont.-London, 1967.

[12] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259-331.

[13] J.-P. Serre, Quelques applications du théorème de densité de Cheboratev, *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323-401.

[14] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, Vieweg, Braunschweig, 1989.

[15] A. Shlapentokh, *Hilbert's Tenth Problem*, Cambridge University Press, Cambridge, 2007.

[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[17] J. H. Silverman, Wieferich's criterion and the abc-conjecture, *J. Number Theory* **30** (1988), 226-237.

[18] J. H. Silverman, *Advanced Topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

[19] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris A-B* **273** (1971), A238-A241.

[20] I. M. Vinogradov, *The Method of Trigonometric Sums in the Theory of Numbers*, Interscience, London and New York, 1954.

Abstract

Hilbert's tenth problem (abbreviated H10) asks if there is an algorithm which decides for every multivariable polynomial over $\mathbb{Z}$ whether the polynomial has a root over $\mathbb{Z}$. This problem was solved by Yuri Matiyasevich in 1970 by showing that there is no such algorithm. More generally, one can ask for any ring R if there is an algorithm which decides for every multivariable polynomial over R whether it has a root over R. This is called H10 over R.

The emphasis of this thesis is on exploring H10 over subrings of $\mathbb{Q}$. These rings are of great theoretical interest since H10 is still unresolved over $\mathbb{Q}$ and there is hope that the solutions for its subrings might lead to a solution for $\mathbb{Q}$. Further, the general techniques for working with H10 over a ring R are introduced in the thesis.

The first chapter of the thesis is mainly devoted to computability theory which is inevitable when working with H10. Using presentations, the theory of computable functions is extended to rings R. This will be of use when H10 is considered over rings R other than $\mathbb{Z}$. The solution to H10 over $\mathbb{Z}$ is also discussed briefly.

In the second chapter the general problem of H10 over a ring R is discussed. The techniques of *diophantine definition* and *diophantine model* are introduced and it is shown how these techniques can be used to solve H10 over a ring R. There is also a short discussion of a conjecture by Barry Mazur and its consequences for H10 over $\mathbb{Q}$.

The third chapter deals with a theorem by Bjorn Poonen which proves that H10 has a negative solution over certain large subrings of $\mathbb{Q}$. This is proved by showing that these rings have a diophantine model of $\mathbb{Z}$. The diophantine model is constructed from an elliptic curve E over $\mathbb{Q}$ with the property that $E(\mathbb{Q}) \cong \mathbb{Z}$. On that account a certain amount of theory of elliptic curves is also introduced in this chapter.

In the fourth chapter a similar theorem of Kirsten Eisenträger and Graham Everest is discussed. It proves that there subrings R_1, R_2 of $\mathbb{Q}$ such that $R_1 \cdot R_2 = \mathbb{Q}$ and that H10 has a negative answer both over R_1 and R_2. These rings are also complementary in a strong sense. Again, the result is proved by constructing a diophantine model of $\mathbb{Z}$ from an elliptic curve.

Zusammenfassung

Hilberts zehntes Problem (abgekürzt H10) ist die Frage, ob es einen Algorithmus gibt, der für jedes multivariable Polynom über $\mathbb{Z}$ entschiedet, ob das Polynom eine Nullstelle über $\mathbb{Z}$ hat. Dieses Problem wurde 1970 von Yuri Matiyasevich gelöst, indem er gezeigt hat, dass kein solcher Algorithmus existiert. Allgemeiner kann man für jeden Ring R fragen, ob es einen Algorithmus gibt, der für jedes multivariable Polynom über R entschiedet, ob es eine Nullstelle über R hat. Dieses Problem heißt H10 über R.

Der Schwerpunkt der Diplomarbeit liegt darauf, H10 über Unterringen von $\mathbb{Q}$ zu untersuchen. Diese Ringe haben große theoretische Bedeutung, da H10 über $\mathbb{Q}$ noch ungelöst ist und die Hoffnung besteht, dass Lösungen für die Unterringe zu einer Lösung für $\mathbb{Q}$ führen könnten. Weiters werden in der Diplomarbeit die allgemeinen Techniken eingeführt, die bei der Arbeit mit H10 über einem Ring R Verwendung finden.

Das erste Kapitel der Diplomarbeit ist hauptsächlich der Berechenbarkeitstheorie gewidmet, die für die Arbeit mit H10 unabdingbar ist. Über Darstellungen wird die Theorie berechenbarer Funktionen auf Ringe R ausgeweitet. Diese wird benötigt, wenn H10 über einem anderen Ring als $\mathbb{Z}$ betrachtet wird. Auch die Lösung von H10 über $\mathbb{Z}$ wird kurz diskutiert.

Im zweiten Kapitel wird das allgemeine Problem H10 über einem Ring R diskutiert. Die Techniken der *diophantischen Definition* und des *diophantischen Modells* werden eingeführt und es wird gezeigt, wie diese verwendet werden können, um H10 über einem Ring R zu lösen. Eine Vermutung von Barry Mazur und ihre Konsequenzen für H10 über $\mathbb{Q}$ werden ebenfalls kurz diskutiert.

Das dritte Kapitel behandelt einen Satz von Bjorn Poonen, der beweist, dass H10 über bestimmten großen Unterringen von $\mathbb{Q}$ eine negative Lösung hat. Dies wird über die Konstruktion eines diophantischen Modells von $\mathbb{Z}$ in diesen Ringen gezeigt. Das diophantische Modell wird über eine elliptische Kurve E über $\mathbb{Q}$ mit der Eigenschaft $E(\mathbb{Q}) \cong \mathbb{Z}$ konstruiert. Dafür wird eine gewisse Menge Theorie elliptischer Kurven in diesem Kapitel eingeführt.

Im vierten Kapitel wird ein ähnlicher Satz von Kirsten Eisenträger und Graham Everest diskutiert. Der Satz beweist die Existenz von Unterringen R_1, R_2 von $\mathbb{Q}$, für die $R_1 \cdot R_2 = \mathbb{Q}$ gilt und über denen H10 eine negative Antwort hat. Weiters sind diese Ringe in einem starken Sinn komplementär. Auch dieses Resultat wird bewiesen, indem ein diophantisches Modell von $\mathbb{Z}$ über eine elliptische Kurve konstruiert wird.

Lebenslauf

Name:	Stefan Perlega
Geburtsdatum:	13. April 1985
Geburtsort:	Oberndorf bei Salzburg

Ausbildung:	
1995-2003	Musisches Gymnasium Salzburg
2005-2011	Diplomstudium Mathematik an der Universität Wien

Arbeit:	
10/2003-09/2004	Zivildienst für das Österreichische Rote Kreuz
10/2008-01/2009	Tutor an der Universität Wien