TN520
Altezze ed equazioni diofantee
Heights and diophantine equations
Università degli Studi Roma 3
A.A. 2022/2023

Fabrizio Barroero

May 26, 2023

Contents

Foreword

This script is based on a course about Diophantine equations and heights given by Prof. Philipp Habegger at the University of Basel in 2018.
Please notify me of any mistake/typo you find or if you think some point need some clarification.

1 Introduction

In this course are going to get to know a new tool to solve (or better just "say something about") diophantine equations: the Weil height. In this chapter we define the height of rational numbers, see some basic properties and an application.
In order to define the height of algebraic numbers we need to recall some basic algebraic number theory, which will be done in Chapter 2. After this we are going to define the Weil height and prove several important properties.
All of this is going to take a big part of the course. For the rest of the course we are going to treat some diophantine problems with the help of this tool.

1.1 What is the height?

The basic question is the following: how can one measure the "complexity" of rational numbers? Here is some homework. One should try to order the following list of rational numbers by their complexity:

$$5/7, \quad 1, \quad 1/2023, \quad 200, \quad 1985/1986, \quad 1.000.000/2.000.000, \quad 1.000.000/2.000.001.$$

Now, it is a priori not clear how one can measure this complexity. One natural measure could be the number of bits a computer needs to store these numbers. This consideration leads to the following definition.

Definition 1.1.1. Let $x = a/b \in \mathbb{Q}$ with coprime $a, b \in \mathbb{Z}$ and $b \geq 1$. The **Weil height** or just **height** of x is

$$h(x) = \log \max\{|a|, b\}.$$

Example 1.1.2. We have

$$h(5/7) = \log 7, \quad h(1) = 0, \quad h(1/2023) = \log 2023, \quad h(1985/1986) = \log 1986$$

and

$$h(1.000.000/2.000.000) = \log 2, \quad h(1.000.000/2.000.001) = \log(2.000.001)$$

Remark 1.1.3. Up to a multiplicative factor $h(x)$ is the number of bits that a computer needs to store the rational number x.
We sometimes also work with the exponential height $H(x) = e^{h(x)} = \max\{|a|, b\}$.

Let us see some basic facts about the height.

Lemma 1.1.4. *For all $x, y \in \mathbb{Q}$ we have the following properties.*

(i) *We have $h(x) \geq 0$ and equality holds exactly when $x = 0$ or $x = \pm 1$.*

(ii) *For $x \neq 0$ and $k \geq 0$ is an integer, we have $h(x^k) = kh(x)$.*

(iii) *For $x \neq 0$ we have $h(x^{-1}) = h(x)$, and by (ii) it follows that $h(x^k) = |k|h(x)$ for all $k \in \mathbb{Z}$.*

(iv) *We have $h(xy) \leq h(x) + h(y)$ and $h(\pm x) = h(x)$.*

(v) *We have $h(x + y) \leq h(x) + h(y) + \log 2$.*

(vi) *For all real numbers B the set*

$$\{x \in \mathbb{Q} : h(x) \leq B\}$$

is finite.

Proof. The first four facts are trivial and left as an exercise. We are actually going to prove them in much greater generality.
We start with (v).
Let $x = a/b$ and $y = c/d$ with $a, b \in \mathbb{Z}$ coprime and $c, d \in \mathbb{Z}$ also coprime and $b \geq 1, d \geq 1$. We have

$$x + y = \frac{p}{q} \quad \text{with} \quad p = ad + bc \text{ and } q = bd \geq 1.$$

Even if p, q are integers they are not coprime in general and we cannot conclude that $h(x + y)$ equals $\log \max\{|p|, q\}$. At least $h(x + y) \leq \log \max\{|p|, q\}$ holds for sure and this is enough for us. Indeed, $|p| \leq |a|d + |c|b \leq 2 \max\{|a|, b\} \max\{|c|, d\}$ and $q \leq \max\{|a|, b\} \max\{|c|, d\}$ and then (v) follows by

$$\log \max\{|p|, q\} \leq \log \max\{|a|, b\} + \log \max\{|c|, d\} + \log 2 = h(x) + h(y) + \log 2.$$

Part (vi) is even easier. If $h(x) \leq B$ with $x = a/b$ as above, then $\max\{|a|, b\} \leq e^B$. Since the numerator and the denominator of x are bounded, there are at most finitely many possibilities for them and therefore finitely many x. □

Remark 1.1.5. Note that properties (ii), (iii) and (iv) suggest that the height is "compatible" with the multiplicative group $\mathbb{Q}^\times$.

1.2 An example

We see how we can use the height we have just defined to find the solutions $x \in \mathbb{Q}$ of the equation

$$x^n + x^m + 1 = 0, \tag{1.1}$$

where $n > m > 0$ are integers. This equation has three unknowns (n, m, x).
Note that, in general, the polynomial $X^n + X^m + 1$ is not irreducible in $\mathbb{Q}$. For instance we have $X^5 + X^4 + 1 = (X^2 + X + 1)(X^3 - X + 1)$.
Even if there is really no need to employ it, we use the height to show that there are actually no solutions. We consider two cases.

Case 1: $n \geq 2m$. We have $x^n = -x^m - 1$ and this implies $h(x^n) = h(-x^m - 1)$. We use the properties of heights we have seen in Lemma 1.1.4. By (ii) we have $h(x^n) = nh(x)$ and by (v) we have $h(-x^m - 1) \leq h(-x^m) + h(-1) + \log 2$. But $h(-1) = 0$ and $h(-x^m) = h(x^m) = mh(x)$ By (i), (ii) and (iv). It follows that

$$nh(x) \leq mh(x) + \log 2 \quad \text{and thus} \quad h(x) \leq \frac{m}{n}h(x) + \frac{\log 2}{n} \leq \frac{1}{2}h(x) + \frac{\log 2}{2}.$$

We conclude that $h(x) \leq \log 2$. The only rational numbers with height $\leq \log 2$ are

$$0, \pm 1, \pm 2, \pm\frac{1}{2},$$

and one easily checks that they are not solutions.
Case 2: $n < 2m$. Since $x \neq 0$ we may divide by x^n and obtain $1 + y^{n-m} + y^n = 0$, where $y = 1/x$. Note that $n - m < n - n/2 = n/2$, and thus $n > 2(n - m)$. We are back in case 1, with y in place of x. So we are done.

2 Elements of Algebraic Number Theory

In this chapter we give a brief overview on basic concepts of algebraic number theory, which we are going to need in order to define and works with the Weil height.
For more details we refer to [1], [6], [4], [7] and [8].

2.1 Field extensions

In this section we introduce notations and recall some facts about fields and field extensions.
Let K be a field and $F \subseteq K$ a subring that is also a field. We say that K/F is a **field extension** and that F is a **subfield** of K.
One can see K as a vector space over F (or an F-vector space). Then, K has a basis as an F-vector space. We are interested in the case when the dimension is finite.

Definition 2.1.1. Let K/F a field extension. If K is a finite-dimensional F-vector space we say that K/F is a **finite field extension** and we call

$$[K : F] = \dim_F K$$

the **degree of the extension**. We also say that K is a **finite extension** of F.

Definition 2.1.2. Let K/F a field extension and let $x \in K$ be an element that is algebraic over F. We call **minimal polynomial** of x over F a monic polynomial $P \in F[X]$ of minimal degree such that $P(x) = 0$.

Proposition 2.1.3. *An $x \in K$ that is algebraic over a subfield F of K has a unique minimal polynomial P over F and P is irreducible.*

Let K/F be a finite extension of fields of characteristic 0. We recall the following theorems. For a proof we refer to [7].

Theorem 2.1.4 (Primitive Element Theorem)**.** *There exists $x \in K$ with $K = F(x)$. In other words, there exists a polynomial $P \in F[X]$ such that K is isomorphic to $F[X]/(P)$.*

Theorem 2.1.5. *Let x and P as in the above theorem and let L/F be a field extension such that P splits in linear factors in $L[X]$[1]. There are exactly $d = [K : F]$ pairwise distinct embeddings $\sigma_1, \ldots, \sigma_d : K \to L$, such that $\sigma_i|_F$ is the inclusion $F \hookrightarrow L$.*

[1]This is the case, for instance, if L is algebraically closed, e.g., when $L = \mathbb{C}$.

Example 2.1.6. We consider the following examples.

(i) We take $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{5})$ and $L = \mathbb{C}$. Then, $[K : \mathbb{Q}] = 2$ and the two embeddings $\sigma_{1,2} : K \to \mathbb{C}$ are given by $\sigma_1(\sqrt{5}) = \sqrt{5}$ and $\sigma_2(\sqrt{5}) = -\sqrt{5}$.

(ii) We now set $F = \mathbb{Q}, K = \mathbb{Q}(2^{1/3})$ and again $L = \mathbb{C}$. Since $[K : \mathbb{Q}] = 3$, there are three embeddings $\sigma_1, \sigma_2, \sigma_3 : K \to \mathbb{C}$, given by

$$\sigma_1(2^{1/3}) = 2^{1/3}, \quad \sigma_1(2^{1/3}) = 2^{1/3}e^{2\pi i/3} \quad \text{and} \quad \sigma_1(2^{1/3}) = 2^{1/3}e^{4\pi i/3}.$$

Exercise 2.1.7. Prove the following fact. Recall the setting of Theorem 2.1.5. Consider a field K' such that $F \subseteq K' \subseteq K$. Then, each embedding $K' \to L$ can be extended in exactly $[K : K']$ different ways to an embedding $K \to L$.

The hypothesis of the above theorems that F should have characteristic 0 can be weakened. We must assume that K/F is a separable field extension. For instance, this holds when F is a finite field.
In this course the field $\mathbb{Q}$ of rational numbers and its finite extensions play a special role.

Definition 2.1.8. A finite extension of $\mathbb{Q}$ is called **number field**. The degree of a number field is $[K : \mathbb{Q}]$.

Example 2.1.9. Let us see a couple of examples.

(i) Clearly, $\mathbb{Q}$ is a number field itself.

(ii) The polynomial $X^2 + 1$ is irreducible in $\mathbb{Q}[X]$. Therefore, $K = \mathbb{Q}[X]/(P) = \mathbb{Q}(\sqrt{-1})$ is a number field and $K/\mathbb{Q}$ has degree 2. Here $\sqrt{-1}$ is a symbol for the coset $X + (P)$.

(iii) The field of real numbers $\mathbb{R}$ is not a number field. If $\mathbb{R}/\mathbb{Q}$ was a finite extension, $\mathbb{R}$ would be isomorphic to $\mathbb{Q}^n$ as a $\mathbb{Q}$-vector space, for some $n \in \mathbb{N}$. Then, $\mathbb{R}$ would be countable and we know that that is not the case. For the same reason $\mathbb{C}$ cannot be a number field.

(iv) A number field K is called **quadratic** if $[K : \mathbb{Q}] = 2$. Quadratic fields are simple non-trivial examples of number fields.
Let $m \in \mathbb{N} \setminus \{0, 1\}$ be a squarefree number, i.e., such that there is no prime number p so that $p^2 \mid m$. The polynomial

$$P = X^2 - m \in \mathbb{Q}[X]$$

is then irreducible, for instance because of Eisenstein criterium. The quotient $\mathbb{Q}[X]/(P)$ is a field K and we have $[K : \mathbb{Q}] = 2$ and

$$K = \mathbb{Q}(\sqrt{m})$$

where $\sqrt{m}$ is the coset $X + (P) \in K$.
A basis of K as a $\mathbb{Q}$-vector space is $(1, \sqrt{m})$. In other words, all elements $x \in K$ can be written uniquely as a linear combination $x = a + b\sqrt{m}$ with $a, b \in \mathbb{Q}$.
We now see that all quadratic field extensions are of the form $\mathbb{Q}(\sqrt{m})$. Let $K/\mathbb{Q}$ be a quadratic extension. There exist $x \in K$ with $x \notin \mathbb{Q}$. As $\dim_{\mathbb{Q}} K = 2$, the

elements $(1, x, x^2)$ are linearly dependent over $\mathbb{Q}$. There are $a, b, c \in \mathbb{Q}$, not all 0, with $ax^2 + bx + c = 0$. As $x \notin \mathbb{Q}$ we must have $a \neq 0$ and we can assume $a = 1$ without loss of generality. Completing the square we get $(x + b/2)^2 + c - b^2/4 = 0$ and this implies $K = \mathbb{Q}((b^2/4-c)^{1/2})$. Finally, we can multiply the rational number $b^2/4 - c$ with a y^2, where $y \in \mathbb{Q} \setminus \{0\}$ and get a squarefree integer m that satisfies $K = \mathbb{Q}(m^{1/2})$. Clearly $m \neq 0, 1$.

(v) Eisenstein's criterion implies that $X^3 - 2$ is an irreducible polynomial in $\mathbb{Q}[X]$. The field $\mathbb{Q}(2^{1/3})$ is a number field of degree 3.

2.2 Rings of integers in number fields

The aim of this section is to introduce the "correct" generalization $\mathcal{O}_K$ of the ring of rational integers $\mathbb{Z}$ in a number field K. For instance in the case $K = \mathbb{Q}(\sqrt{-1})$ we will see that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}]$. Unfortunately, it is not always that easy. For instance, $\mathcal{O}_K = \mathbb{Z}[(\sqrt{5} + 1)/2]$ for $K = \mathbb{Q}(\sqrt{5})$.
The construction is a general concept in commutative algebra. For us rings are commutative and have 1.

Definition 2.2.1. Let B be a ring and A a subring of B. The subset of B defined as

$$A_B = \{x \in B : \text{there exist } d \in \mathbb{Z}^{>0} \text{ and } a_1, \ldots, a_d \in A \text{ with } x^d + a_1 x^{d-1} + \cdots + a_d = 0\}$$

is called the **integral closure** of A in B. Elements of A_B are called **integral** over A. In case $A = \mathbb{Z}$ and $B = K$ is a number field we will often use the notation $\mathcal{O}_K$ for $\mathbb{Z}_K$.

Note that $A \subseteq A_B$, as all $a \in A$ are roots of $X - a \in A[X]$.
Before we explain some properties of A_B, we consider the first example: $A = \mathbb{Z}$ and $B = \mathbb{Q}$.

Exercise 2.2.2. Prove that $\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$.

We are not going to prove the following fact.

Proposition 2.2.3. *Let B be a ring and A a subring of B. Then, A_B is a subring of B.*

Now we come to an important definition.

Definition 2.2.4. Let K be a number field. We call $\mathbb{Z}_K = \mathcal{O}_K$ the **ring of algebraic integers** in K. Elements of $\mathcal{O}_K$ are called **integers** of K.

A large part of a course in algebraic number theory is dedicated to studying properties of this ring. We are only going to see what we need for defining the height.

Example 2.2.5. We have seen in Exercise 2.2.2 that $\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$. Note that the exact same argument shows that $\mathbb{Z}_K \cap \mathbb{Q} = \mathbb{Z}$ for all fields $K \supseteq \mathbb{Q}$. Therefore, one gets nothing new in the case $K = \mathbb{Q}$, as one would of course expect. On the other hand, we have $\mathcal{O}_K \supsetneq \mathbb{Z}$ for all number fields K with $K \neq \mathbb{Q}$. Indeed, for any $\alpha \in K \setminus \mathbb{Q}$ we have $a\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ where a is the least common multiple of the denominators of the coefficients of the minimal polynomial of α.

Example 2.2.6. It is easy to see that $a + b\sqrt{d}$ is an integer of $\mathbb{Q}(\sqrt{d})$, for $a, b \in \mathbb{Z}$. Moreover, note that the golden ratio $(1 + \sqrt{5})/2$ is an integer since it is a root of $X^2 - X - 1$.

Remark 2.2.7. The ring $\mathbb{Z}_{\mathbb{C}}$ is well-defined. It is called the **ring of algebraic integers**, but it will not play any major role in this course.

Let K be a number field and $x \in K$. The minimal polynomial $P \in \mathbb{Q}[X]$ of x over $\mathbb{Q}$ is monic and satisfies $P(x) = 0$. The coefficients of P are not necessarily integers, so we cannot conclude that x is in $\mathcal{O}_K$, Otherwise we would have $K = \mathcal{O}_K$. If $P \in \mathbb{Z}[X]$, then $x \in \mathcal{O}_K$ by definition. In the next Lemma we prove the converse.

Lemma 2.2.8. *Let K be a number field and $x \in K$ be an element of K. Let $P \in \mathbb{Q}[X]$ be the minimal polynomial of x over $\mathbb{Q}$. Then, $x \in \mathcal{O}_K$ if and only if $P \in \mathbb{Z}[X]$.*

Proof. The implication "$\Leftarrow$" follows by definition. Let now $x \in \mathcal{O}_K$. There exists $R = X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$ with $R(x) = 0$. We cannot assume that R is the minimal polynomial of x over $\mathbb{Q}$. In any case, R lies in the ideal $\{Q \in \mathbb{Q}[X] : Q(x) = 0\}$ and this ideal is generated by P. Therefore P divides R in the ring $\mathbb{Q}[X]$, i.e., we have $R = PQ$ for some $Q \in \mathbb{Q}[X]$. Since P and Q are monic, there are positive $p, q \in \mathbb{Z}$ such that $pP, qQ \in \mathbb{Z}[X]$ are primitive, i.e., their coefficients are coprime. Gauss' Lemma then implies that $(pP)(qQ) = pqR$ is also primitive. But this is only possible if $pq = \pm 1$. It then follows that $p = \pm 1$ and thus P has coefficients in $\mathbb{Z}$. □

Example 2.2.9. This lemma implies that algebraic numbers like $\sqrt{3}/2$, $\sqrt{5}/2$, $(2 + \sqrt{7})/3$ are not integers.

Example 2.2.10. We now describe $\mathcal{O}_K$ for the simplest non-trivial number fields: quadratic extensions of $\mathbb{Q}$.
Let $m \in \mathbb{Z} \setminus \{0, 1\}$ be squarefree, i.e., no square of a prime number divides m. Clearly we have $m \not\equiv 0 \pmod 4$. We know that all quadratic extensions of $\mathbb{Q}$ have the form $K = \mathbb{Q}(\sqrt{m})$ for some such m.
We want to determine $\mathcal{O}_K$. The residue class of m modulo 4 plays an important role here. We have $m \equiv 1, 2, \text{ or } 3 \pmod 4$.
Since $X^2 - m$ is monic and has integer coefficients we have $\sqrt{m} \in \mathcal{O}_K$. As $\mathcal{O}_K$ is a ring, it follows that $\mathbb{Z}[\sqrt{m}] = \mathbb{Z} + \sqrt{m}\mathbb{Z} \subseteq \mathcal{O}_K$.
All elements $x \in K$ have the form $a + \sqrt{m}b$ with uniquely determined $a, b \in \mathbb{Q}$.
We take now $x \in \mathcal{O}_K$ and find some restrictions on a, b. If $b = 0$, then $x = a \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$, so we assume $b \neq 0$ so that $x \notin \mathbb{Q}$. We have $m = ((x - a)/b)^2$ and a quick calculation shows that

$$P = X^2 - 2aX + (a^2 - b^2 m) \in \mathbb{Q}[X]$$

has x as a root. Since $x \notin \mathbb{Q}$, the polynomial P must be irreducible and is then the minimal polynomial of x over $\mathbb{Q}$. By "$\Rightarrow$" of Lemma 2.2.8 we know that $P \in \mathbb{Z}[X]$. In other words, $a' = 2a, a^2 - b^2 m \in \mathbb{Z}$. Thus, $4(a^2 - b^2 m) = a'^2 - 4b^2 m \in 4\mathbb{Z}$ and so

$(2b)^2 m \in \mathbb{Z}$. Since m is a squarefree integer, it follows that $b' = 2b \in \mathbb{Z}$. We then have $a'^2 - b'^2 m \in 4\mathbb{Z}$ or

$$a'^2 \equiv b'^2 m \pmod 4. \tag{2.1}$$

If a' is odd, we have $a'^2 \equiv 1 \pmod 4$ and thus $b'^2 m \equiv 1 \pmod 4$. So b' must also be odd and $m \equiv 1 \pmod 4$.
In case $m \equiv 2, 3 \pmod 4$ we must then have that a' is even. From (2.1) it follows that $0 \equiv b'^2 m \pmod 4$ and so b' must be even, as well. In this case a and b are in $\mathbb{Z}$ and we can conclude that all elements of $\mathcal{O}_K$ lie in $\mathbb{Z} + \sqrt{m}\mathbb{Z}$. We already know that the other inclusion holds, so

$$\mathcal{O}_K = \mathbb{Z} + \sqrt{m}\mathbb{Z} = \mathbb{Z}[\sqrt{m}] \quad \text{if} \quad m \equiv 2, 3 \pmod 4. \tag{2.2}$$

We are left with the case $m \equiv 1 \pmod 4$. This implies that $a' - b'$ is even. But $a - b = (a' - b')/2 \in \mathbb{Z}$ and so $(a' - b')/2 + b'(1 + \sqrt{m})/2 = a + b\sqrt{m} = x$. We find $\mathcal{O}_K \subseteq \mathbb{Z} + (1 + \sqrt{m})/2\mathbb{Z}$. On the other hand, it is easy to show that $(1 + \sqrt{m})/2$ is integral over $\mathbb{Z}$ because its minimal polynomial is $X^2 - X + (1 - m)/4 \in \mathbb{Z}[X]$. Finally,

$$\mathcal{O}_K = \mathbb{Z} + \frac{1 + \sqrt{m}}{2}\mathbb{Z} = \mathbb{Z}\left[\frac{1 + \sqrt{m}}{2}\right] \quad \text{if} \quad m \equiv 1 \pmod 4. \tag{2.3}$$

Remark 2.2.11. If K is a number field, in general there is no $x \in \mathcal{O}_K$ such that $\mathcal{O}_K = \mathbb{Z}[x]$.

Proposition 2.2.12. *Let K a number field and $x \in K$, where $a_0 x^m + \cdots + a_m = 0$ with $a_0, \ldots, a_m \in \mathbb{Z}$ and $a_0 \neq 0$. Then we have $a_0 x \in \mathcal{O}_K$. In particular, for all $x \in K$ there is an $a \in \mathbb{Z} \setminus \{0\}$ such that $ax \in \mathcal{O}_K$ and K is the quotient field of $\mathcal{O}_K$.*

Proof. We multiply $a_0 x^m + a_1 x^{m-1} + \cdots + a_m = 0$ with a_0^{m-1} and get $(a_0 x)^m + a_1 (a_0 x)^{m-1} + a_2 a_0 (a_0 x)^{m-2} + \cdots + a_{m-1} a_0^{m-2} (a_0 x) + a_m a_0^{m-1} = 0$. Therefore $a_0 x$ is a root of a monic polynomial with coefficients in $\mathbb{Z}$ and so $a_0 x \in \mathcal{O}_K$ by definition of $\mathcal{O}_K$. The second statement follows from the first as an arbitrary $x \in K$ is a root of a polynomial in $\mathbb{Z}[X]$. □

2.3 Unique factorization

Now that we have seen some examples of ring of integers we may ask ourselves: are they PID like $\mathbb{Z}$?

Example 2.3.1. Let $K = \mathbb{Q}(\sqrt{-5})$. We know form Example 2.2.10 that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. In this example we see that the ring $\mathcal{O}_K$ is not a UFD (and therefore not a PID) by looking at the factorization

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

We show that 2 is not a prime element of $\mathcal{O}_K$ but it is irreducible. Therefore, $\mathcal{O}_K$ cannot be a UFD.

We certainly have $2 \mid (1+\sqrt{-5})(1-\sqrt{5})$, but

$$\frac{1 \pm \sqrt{-5}}{2} = \frac{1}{2} \pm \frac{\sqrt{-5}}{2} \notin R.$$

Therefore, $2 \nmid (1+\sqrt{-5})$ and $2 \nmid (1-\sqrt{-5})$ and so 2 is not prime in $\mathcal{O}_K$.
We now show that 2 is irreducible in $\mathcal{O}_K$. We assume that

$$2 = (a+\sqrt{-5}b)(c+\sqrt{-5}d) \tag{2.4}$$

for some $a, b, c, d \in \mathbb{Z}$. We use complex conjugation and get $2 = (a-\sqrt{-5}b)(c-\sqrt{-5}d)$. We combine this with (2.4) and get

$$4 = (a+\sqrt{-5}b)(a-\sqrt{-5}b)(c+\sqrt{-5}d)(c-\sqrt{-5}d) = (a^2+5b^2)(c^2+5d^2).$$

Both factors on the rightmost side are integers, both positive. We use the fact that $\mathbb{Z}$ is a UFD and conclude that $a^2+5b^2 \in \{1,2,4\}$. This implies $b=0$ and $a=1$ or 2. If we now substitute this in (2.4) we get $d=0$ and $c=2$ or 1. In any case, one of the two factors in (2.4) is invertible and so 2 is an irreducible element of $\mathcal{O}_K$.

We are going to see that in ring of integers there is another kind of unique factorization.

Definition 2.3.2. Let R be a ring (as always commutative with 1). We define the **sum** of the two ideals $I, J \subseteq R$ as

$$I + J = \{a+b : a \in I \text{ and } b \in J\}.$$

We can also define their **product** as

$$IJ = \left\{ \sum_{i=1}^{n} a_i b_i : a_1, \ldots, a_n \in I \text{ and } b_1, \ldots, b_n \in J \right\}.$$

Lemma 2.3.3. *The sum and the product of two ideals is an ideal of R.*

Proof. This proof is left as an exercise. □

Example 2.3.4. We see some examples.

(i) Let R be a ring and I, J be ideals of R. If $I = aR$ and $J = bR$ with $a, b \in R$ are principal ideals, then clearly $IJ = abR$.

(iii) Every integer $n \in \mathbb{Z} \setminus \{0\}$ is a product $\pm p_1^{e_1} \cdots p_g^{e_g}$ with $p_1, \ldots, p_g$ pairwise distinct prime numbers and $e_1, \ldots, e_g \in \mathbb{N}$. Considering the corresponding principal ideals we get

$$n\mathbb{Z} = (p_1\mathbb{Z})^{e_1} \cdots (p_g\mathbb{Z})^{e_g}.$$

As all $p_i\mathbb{Z}$ are generated by a prime number, they must be prime ideals. Therefore, we can write all non-zero ideals of $\mathbb{Z}$ as product of prime ideals. Since $\mathbb{Z}$ is a PID, one can conclude that this factorization is unique up to the order.

Remark 2.3.5. The following properties can easily be verified.

(i) These two operations are associative and commutative and they satisfy the distributive property.

(ii) The zero ideal is a neutral element with respect to addition and the trivial ideal R is a neutral element with respect to multiplication.

In general the set of ideals of a ring with addition is not a group as inverses are missing.

We now state a very important property of rings of integers in number fields.

Theorem 2.3.6. *Let $\mathcal{O}_K$ be the ring of integer of the number field K. All proper ideals $I \neq 0$ of $\mathcal{O}_K$ are product of finitely many non-zero prime ideals of $\mathcal{O}_K$. Moreover, this factorization is unique up to the order. In other words, there exist pairwise distinct prime ideals $P_1, \dots, P_g$ different form 0 and positive integers $e_1, \dots, e_g$ with $I = P_1^{e_1} \cdots P_g^{e_g}$. If $Q_1, \dots, Q_h$ are pairwise distinct prime ideals and $f_1, \dots, f_h$ positive integers with $I = Q_1^{f_1} \cdots Q_h^{f_h}$, then $g = h$ and after permuting the Q_i we have $P_i = Q_i$ and $e_i = f_i$ for all $1 \leq i \leq g$.*

The proof of this statement is not hard but a bit lengthy and technical. It is a central theorem in the Algebraic Number Theory course. Let us see an example.

Example 2.3.7. We consider again $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. We have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}). \tag{2.5}$$

One can easily prove that $2, 3, 1 \pm \sqrt{-5}$ are irreducible as elements of $\mathcal{O}_K$.
Equality (2.5) holds also for the corresponding principal ideals

$$6\mathcal{O}_K = 2\mathcal{O}_K 3\mathcal{O}_K = (1 + \sqrt{-5})\mathcal{O}_K(1 - \sqrt{-5})\mathcal{O}_K.$$

This factorization does not contradict the above theorem as $2\mathcal{O}_K, 3\mathcal{O}_K, (1 \pm \sqrt{-5})\mathcal{O}_K$ are <u>not</u> prime ideals. Indeed, they can be further factored:

$$2\mathcal{O}_K = P^2 \quad \text{and} \quad 3\mathcal{O}_K = Q_1 Q_2$$

where

$$P = 2\mathcal{O}_K + (1+\sqrt{-5})\mathcal{O}_K, \quad Q_1 = 3\mathcal{O}_K + (1+\sqrt{-5})\mathcal{O}_K \quad \text{and} \quad Q_2 = 3\mathcal{O}_K + (1-\sqrt{-5})\mathcal{O}_K.$$

With some computations one can verify the above equalities. As an example we verify $P^2 = 2\mathcal{O}_K$. We have

$$P^2 = 4\mathcal{O}_K + 2(1+\sqrt{-5})\mathcal{O}_K + (1+\sqrt{-5})^2\mathcal{O}_K = 4\mathcal{O}_K + 2(1+\sqrt{-5})\mathcal{O}_K + 2(-2+\sqrt{-5})\mathcal{O}_K$$

As $4, 2(1 + \sqrt{-5}), 2(-2 + \sqrt{-5}) \in 2\mathcal{O}_K$, we get $P^2 \subseteq 2\mathcal{O}_K$. On the other hand $6 = 2(1 + \sqrt{-5}) - 2(-2 + \sqrt{-5}) \in P^2$ and thus $2 = 6 - 4 \in P^2$. As P^2 is an ideal, it follows that $2\mathcal{O}_K \subseteq P^2$ and so $2\mathcal{O}_K = P^2$.
One can prove that P, Q_1 and Q_2 are prime ideals and that they are not principal.
Moreover, one can easily verify that

$$(1 + \sqrt{-5})\mathcal{O}_K = PQ_1 \quad \text{and} \quad (1 - \sqrt{-5})\mathcal{O}_K = PQ_2.$$

Exercise 2.3.8. Let P be a prime ideal of $\mathcal{O}_K$. Prove that $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

We now introduce a the concept of divisibility between ideals. Note that this makes sense in any ring.

Definition 2.3.9. Let $\mathcal{O}_K$ be the ring of integer of the number field K and I, J ideals of $\mathcal{O}_K$. We say that I **divides** J and we write $I \mid J$ if there exists an ideal I' of $\mathcal{O}_K$ with $II' = J$.

Proposition 2.3.10 ("To divide is to contain")**.** *Let $\mathcal{O}_K$ be the ring of integer of the number field K and I, J be ideals of $\mathcal{O}_K$. Then*

$$I \mid J \quad \Longleftrightarrow \quad J \subseteq I.$$

As we said above, $\mathcal{O}_K$ is in general not a PID. On the other hand, one of the central theorems in algebraic number theory says that an ideal of $\mathcal{O}_K$ is "not too far" from being principal. We see now a corollary of this important result.

Corollary 2.3.11. *Let I be an ideal of $\mathcal{O}_K$. There exists a postive integer n such that I^n is principal.*

2.4 The norm of an ideal

Definition-Lemma 2.4.1. Let K be a number field and $I \neq 0$ be an ideal of $\mathcal{O}_K$. Then, $\mathcal{O}_K/I$ is a finite ring. We define the **norm** of I as the cardinality

$$N(I) = \#(\mathcal{O}_K/I) < \infty.$$

We set $N(0) = 0$ for the zero ideal.

Example 2.4.2. Let us see some easy examples.

(i) Let $K = \mathbb{Q}$, then $\mathbb{Z}_{\mathbb{Q}} = \mathbb{Z}$ and all ideals of $\mathbb{Z}$ have the form $n\mathbb{Z}$ for a $n \in \mathbb{Z}$. For $n \neq 0$, the quotient $\mathbb{Z}/n\mathbb{Z}$ is a ring with $|n|$ elements. We then get $N(n\mathbb{Z}) = |n|$ for all $n \in \mathbb{Z}$.

(ii) For $K = \mathbb{Q}(\sqrt{-1})$ we know $\mathcal{O}_K = \mathbb{Z}[\sqrt{-1}] = \mathbb{Z} + \sqrt{-1}\mathbb{Z}$. The principal ideal $2\mathcal{O}_K$ consists of elements $2a + 2b\sqrt{-1}$ with $a, b \in \mathbb{Z}$. Every element of $\mathcal{O}_K$ is the sum of an element of $2\mathcal{O}_K$ plus a number of the form $a + b\sqrt{-1}$ with $a, b \in \{0, 1\}$. Moreover, two different $a + b\sqrt{-1}$ with $a, b \in \{0, 1\}$ cannot belong to the same residue class modulo $2\mathcal{O}_K$. It follows that $\#(\mathcal{O}_K/2\mathcal{O}_K) = N(2\mathcal{O}_K) = 4$.

Definition 2.4.3. Let K be a number field and $x \in K$. We define the **norm** of x to be

$$\mathrm{N}_{K/\mathbb{Q}}(x) = \prod_{\sigma} \sigma(x),$$

where the product is taken over all embeddings $\sigma : K \to \mathbb{C}$.

Exercise 2.4.4. Let K and F be number fields with $F \subseteq K$ and let $x \in F$. Prove that

$$\mathrm{N}_{K/\mathbb{Q}}(x) = \mathrm{N}_{F/\mathbb{Q}}(x)^{[K:F]}$$

With the help of the norm in some situations we can decide whether an ideal is prime or not.

Lemma 2.4.5. *Let K be a number field and $I \subseteq \mathcal{O}_K$ an ideal.*

(i) We have $N(I) \in I$. In particular, a non-zero ideal of $\mathcal{O}_K$ contains a positive rational integer.

(ii) If $N(I)$ is a prime number, then I is a prime ideal.

(iii) The norm of a prime ideal P is a power of p where $p\mathbb{Z} = P \cap \mathbb{Z}$.

(iv) For all $x \in \mathcal{O}_K \setminus \{0\}$ we have

$$N(x\mathcal{O}_K) = |\mathrm{N}_{K/\mathbb{Q}}(x)|.$$

Remark 2.4.6. The converse of Lemma 2.4.5(ii) is false: there are prime ideals whose norm is not a prime number.

Example 2.4.7. Let $K = \mathbb{Q}(\sqrt{-5})$. In Example 2.3.7 we have seen that $2\mathcal{O}_K = P^2$ with $P = 2\mathcal{O}_K + (1+\sqrt{-5})\mathcal{O}_K$. We now want to show that P is a prime ideal. We know $\mathcal{O}_K = \mathbb{Z} + \sqrt{-5}\mathbb{Z}$. Therefore, $2\mathcal{O}_K = 2\mathbb{Z} + 2\sqrt{-5}\mathbb{Z}$ has index 4 in $\mathcal{O}_K$, i.e., $N(2\mathcal{O}_K) = 4$, as we have seen in Example 2.4.2. Since $2\mathcal{O}_K \subseteq P$, we can define a surjective ring homomorphism $\mathcal{O}_K/2\mathcal{O}_K \to \mathcal{O}_K/P$ by $a + 2\mathcal{O}_K \mapsto a + P$. It follows that $N(P) \mid N(2\mathcal{O}_K)$. Therefore, $N(P)$ has to belong to $\{1, 2, 4\}$.
If $N(P) = 1$, then $P = \mathcal{O}_K$ and so $2\mathcal{O}_K = P^2 = \mathcal{O}_K$. This is impossible, for instance because $1/2 \notin \mathcal{O}_K$.
If $N(P) = 4$ the above homomorphism would be an isomorphism. This would imply $2\mathcal{O}_K = P$, and thus $P = P^2$ because $2\mathcal{O}_K = P^2$. This contradicts the unique factorization in prime ideals in Theorem 2.3.6.
Then $N(P) = 2$ must hold and by Lemma 2.4.5(ii), we conclude that P is a prime ideal. Similarly, one can show that Q_1, Q_2 in the factorization of $3\mathcal{O}_K$ in Example 2.3.7 are also prime ideals.

Proposition 2.4.8. *Let K be a number field and $I, J \subseteq \mathcal{O}_K$ ideals. Then $N(IJ) = N(I)N(J)$.*

We are still going to need some facts about the behavior of ideals after an extension of number fields.

Definition-Lemma 2.4.9. Let K and F be number fields with $F \subseteq K$. For an ideal $I \subseteq \mathcal{O}_F$ we define

$$I\mathcal{O}_K = \{x \in K : \text{there are } n \geq 0,\ a_1, \ldots, a_n \in I \text{ and } b_1, \ldots, b_n \in \mathcal{O}_K \text{ with } x = a_1b_1 + \cdots + a_nb_n\}.$$

Then $I\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$. It is the smallest ideal of $\mathcal{O}_K$ that contains I.

We can compare the norm of I with the norm of of $I\mathcal{O}_K$.

Lemma 2.4.10. *Let K and F be number fields with $F \subset K$ and I be an ideal of F. Then we have $N(I\mathcal{O}_K) = N(I)^{[K:F]}$.*

Proof. The claim is obvious if $I = 0$. Let then $I \neq 0$.
We first handle the case in which $I = a\mathcal{O}_F$ is principal. Then, we have $I\mathcal{O}_K = a\mathcal{O}_K$. By Lemma 2.4.5(iv) we have $N(a\mathcal{O}_K) = |\mathrm{N}_{K/\mathbb{Q}}(a)|$ and $N(a\mathcal{O}_F) = |\mathrm{N}_{F/\mathbb{Q}}(a)|$. This gives the second and the fourth equality in

$$N(I\mathcal{O}_K) = N(a\mathcal{O}_K) = |\mathrm{N}_{K/\mathbb{Q}}(a)| = |\mathrm{N}_{F/\mathbb{Q}}(a)|^{[K:F]} = N(a\mathcal{O}_F)^{[K:F]} = N(I)^{[K:F]},$$

while the third follows from Exercise 2.4.4.
Let now $I \neq 0$ be an arbitrary ideal of $\mathcal{O}_F$. By Corollary 2.3.11, there is an $n \geq 1$ such that I^n is principal in $\mathcal{O}_F$. By what we have already proved we have $N(I^n\mathcal{O}_K) = N(I^n)^{[F:K]}$. It is clear that $I^n\mathcal{O}_K = (I\mathcal{O}_K)^n$ and, by Proposition 2.4.8 we have that $N(I\mathcal{O}_K)^n = N(I)^{n[F:K]}$. This gives the claim. □

Let K be a number field and $P \subseteq \mathcal{O}_K$ a prime ideal $P \neq 0$. We know that $N(P) \in P$ by Lemma 2.4.5(i) and therefore, $P \cap \mathbb{Z}$ is a non-zero prime ideal of $\mathbb{Z}$. It has then the form $p\mathbb{Z}$ with $p \geq 2$ a prime number. By Proposition 2.3.10 we know that $P \mid p\mathcal{O}_K$. Therefore $p\mathcal{O}_K = P^e I$ for an ideal $I \subset \mathcal{O}_K$ with $P \nmid I$ and an integer $e \geq 1$.
Moreover, the integral domain $\mathcal{O}_K/P$ is finite and p is in the class of 0 in $\mathcal{O}_K/P$. Therefore, $\mathcal{O}_K/P$ has characteristic p and then we must have $N(P) = p^f$ for some integer $f \geq 1$. Note that $f = [\mathcal{O}_K/P : \mathbb{F}_p]$.

Definition 2.4.11. The exponent e of P in the factorization of $p\mathcal{O}_K$ is called **ramification index** of P and is indicated by $e(P)$.
The exponent f in $N(P) = p^f$ is called **residue degree** of P and is indicated by $f(P)$.

We now see an important fact that links the two integers we have just defined with the degree of K.

Lemma 2.4.12. *Let K be a number field and p a prime number. Let $P_1^{e_1} \cdots P_g^{e_g}$ be the prime ideal factorization of $p\mathcal{O}_K$. We have*

$$\sum_{i=1}^{g} e(P_i)f(P_i) = \sum_{P \mid p\mathcal{O}_K} e(P)f(P) = [K : \mathbb{Q}].$$

2.5 Absolute values

Let K be a number field and $P \neq 0$ be a prime ideal of $\mathcal{O}_K$. We are going to see how to associate to P an absolute value of K.

Definition 2.5.1. In the above notation, let $a \in \mathcal{O}_K \setminus \{0\}$. Then, there is an $e \geq 0$ and an ideal $I \subset \mathcal{O}_K$ with $P \nmid I$, such that $a\mathcal{O}_K = P^e I$. We call

$$\nu_P(a) = e$$

the P**-adic valuation** of a. It is often useful to set $\nu_P(0) = +\infty$.

Remark 2.5.2. Let K a number field and $P \neq 0$ be a prime ideal of $\mathcal{O}_K$. Let $a, b \in \mathcal{O}_K \setminus \{0\}$ with $a\mathcal{O}_K = P^e I$, $b\mathcal{O}_K = P^f J$ and $P \nmid J, P \nmid I$. Then, ν_P satisfies the following properties.

(i) We have $\nu_P(ab) = e + f = \nu_P(a) + \nu_P(b)$ since $ab\mathcal{O}_K = P^{e+f} IJ$ and $P \nmid IJ$. The equality

$$\nu_P(ab) = \nu_P(a) + \nu_P(b) \tag{2.6}$$

holds for all $a, b \in \mathcal{O}_K$, if one adopts the convention $(+\infty) + x = x + (+\infty) = +\infty$ for $x \in \mathbb{R} \cup \{+\infty\}$.

(ii) Let, for instance, $e \leq f$. Then, we have $a \in P^e$ and $b \in P^f \subseteq P^e$. Thus, $a + b \in P^e$ and so $\nu_P(a + b) \geq e = \min\{\nu_P(a), \nu_P(b)\}$.
The inequality

$$\nu_P(a + b) \geq \min\{\nu_P(a), \nu_P(b)\} \tag{2.7}$$

then holds for all $a, b \in \mathcal{O}_K$, if one adopts the convention

$$\min\{+\infty, x\} = \min\{x, +\infty\} = x$$

for all $x \in \mathbb{R} \cup \{+\infty\}$.

We adopt the above conventions about $+\infty$ in the whole Chapter.
We now see how to extend this definition to elements of K.

Remark 2.5.3. If $a \in K \setminus \{0\}$, then, by Proposition 2.2.12, we can write $a = b/c$ for some $b, c \in \mathcal{O}_K$ and we set $\nu_P(a) = \nu_P(b) - \nu_P(c)$.
We should verify that this is well defined. Let $b_1/c_1 = b_2/c_2$ for $b_1, b_2, c_1, c_2 \in \mathcal{O}_K$ with $c_1, c_2 \neq 0$. Then $b_1 c_2 = b_2 c_1$. By (2.6), we have $\nu_P(b_1) + \nu_P(c_2) = \nu_P(b_2) + \nu_P(c_1)$ and thus $\nu_P(b_1/c_1) = \nu_P(b_1) - \nu_P(c_1) = \nu_P(b_2) - \nu_P(c_2) = \nu_P(b_2/c_2)$
We then extend the definition to the whole field K.
It is easy to see that (2.6) extends to elements of K.
Moreover, for $a, b \in K \setminus \{0\}$ there is an $m \in \mathbb{Z}^{>0}$ with $ma, mb \in \mathcal{O}_K$, i.e., (2.7) holds with a, b replaced by ma, mb. An easy computation shows that (2.7) is satisfied for all $a, b \in K$.

Definition 2.5.4. Let K be an arbitrary field. A function $\nu : K \to \mathbb{R} \cup \{+\infty\}$ is called **valuation**, if the following properties are satisfied.

(i) We have $\nu(K^\times) \subseteq \mathbb{R}$.
(ii) For all $x, y \in K$ we have $\nu(xy) = \nu(x) + \nu(y)$.
(iii) For all $x, y \in K$ we have $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$.

The pair (K, ν) is called **valued field**. In the notation, ν is often omitted.

Note that, by definition, if $\nu(K) \neq \{0\}$, we must have $\nu(0) = +\infty$ and $\nu(1) = \nu(-1) = 0$.

Remark 2.5.5. Let (K, ν) be a valued field. Let moreover $\eta > 1$ be a real number. For $x \in K \setminus \{0\}$ we set $|x|_\nu = \eta^{-\nu(x)}$ and $|0|_\nu = 0$. Although this function depends on the choice of η it is not considered in the notation. We call any $|\cdot|_\nu$ associated to the triple (K, ν, η) **absolute value** associated to ν. The number η can be chosen arbitrarily, there are many conventions. This function we have just defined is a genuine absolute value on K, since the properties (i),(ii) and (iii) in the above definition imply the following:

(i) For $x \in K$ we have $|x|_\nu \geq 0$ with equality exactly when $x = 0$.
(ii) For $x, y \in K$ we have $|xy|_\nu = |x|_\nu |y|_\nu$.
(iii) For $x, y \in K$ we have $|x + y|_\nu \leq \max\{|x|_\nu, |y|_\nu\}$.

The inequality in (iii) is stronger than the triangular inequality $|x + y|_\nu \leq |x|_\nu + |y|_\nu$. It is called the **ultrametric inequality**.
In general, an absolute value satisfying the ultrametric inequality is called **non-archimedean**

Example 2.5.6. Let $K = \mathbb{Q}$ and $p \geq 2$ be a prime number. We choose $\eta = p$ and write $\nu_p = \nu_{p\mathbb{Z}}$ and $|\cdot|_p$ for the associated absolute value. Therefore we have $|p|_p = p^{-1}$. If $m \in \mathbb{Z}$ and $p \nmid m$ then we have $|p^e m|_p = |p^e|_p |m|_p = p^{-e}$ for all $e \in \mathbb{Z}$ and $\nu_p(p^e m) = e\nu_p(p) + \nu_p(m) = e$.
Note that ν_p is a discrete valuation and that p is a uniformizer of ν_p.

We now define some absolute values on K. This will be fundamental for the definition of height.

Definition 2.5.7. Let K be a number field and $x \in K$.

(i) Let $x \neq 0$. Fix a prime ideal $P \subset \mathcal{O}_K$ with $P \neq 0$.
Let $e(P)$ be the ramification index of P and $P \cap \mathbb{Z} = p\mathbb{Z}$ with p a prime number. We set
$$|x|_P = p^{-\nu_P(x)/e(P)}. \tag{2.8}$$
and $|0|_P = 0$. We call such an absolute value P**-adic absolute value**. In case $K = \mathbb{Q}$ and $P = p\mathbb{Z}$ we call it p-adic absolute value.

(ii) Let $\sigma : K \to \mathbb{C}$ be a field embedding provided by Theorem 2.1.5. Then we define $|x|_\sigma = |\sigma(x)|$, where $|\cdot|$ is the standard absolute value on $\mathbb{C}$.

Remark 2.5.8. Let $v = P$ be a non-zero prime ideal. Let us justify the choice of constant in (2.8). The ideal $P \cap \mathbb{Z}$ is of the form $p\mathbb{Z}$ for some prime number $p \in \mathbb{Z}$. we have
$$p\mathcal{O}_K = P^{e(P)} I$$
with $P \nmid I$ coprime. Therefore,
$$|p|_P = p^{-\nu_P(p)/e(P)} = p^{-1} = |p|_p.$$
Therefore, $|\cdot|_P$ extends the p-adic absolute value on $\mathbb{Q}$.
Moreover, given a field embedding $\sigma : K \to \mathbb{C}$ the absolute value $|\cdot|_\sigma$ extends the standard absolute value on $\mathbb{Q}$.

Remark 2.5.9. Let K be a number field and $\sigma : K \to \mathbb{C}$ be an embedding. Applying complex conjugation we get another embedding $\overline{\sigma} : K \to \mathbb{C}$, such that $\overline{\sigma}(x) = \overline{\sigma(x)}$ for all $x \in K$.
If σ is not a real embedding we have $\sigma \neq \overline{\sigma}$. In any case we note that $|x|_\sigma = |x|_{\overline{\sigma}}$ for all $x \in K$. In other words σ and $\overline{\sigma}$ define the same absolute value on K.

Example 2.5.10. Let $\alpha = (1+\sqrt{5})/2$ and $K = \mathbb{Q}(\alpha)$. There are two embeddings $\sigma_{1,2} : K \to \mathbb{C}$. We set $\sigma_1(\sqrt{5}) = \sqrt{5}$ and $\sigma_2(\sqrt{5}) = -\sqrt{5}$. Then, $|\alpha|_{\sigma_1} = (1+\sqrt{5})/2$ and $|\alpha|_{\sigma_2} = |(1-\sqrt{5})/2| = (-1+\sqrt{5})/2$. Note that $\alpha \in \mathcal{O}_K^\times$ and therefore α is not contained in any prime ideal of $\mathcal{O}_K$. This means that $|\alpha|_P = 1$ for all non-zero prime ideal P of $\mathcal{O}_K$.

Example 2.5.11. Let $\alpha = 1+\sqrt{-5}$ and $K = \mathbb{Q}(\sqrt{-5})$. There are two embeddings $\sigma_{1,2} : K \to \mathbb{C}$. We set $\sigma_1(\sqrt{-5}) = \sqrt{-5}$ and $\sigma_2(\sqrt{-5}) = -\sqrt{-5}$. As we have observed above $|\cdot|_{\sigma_1} = |\cdot|_{\sigma_2}$. Then $|\alpha|_{\sigma_1} = |1+i\sqrt{5}| = \sqrt{6}$.
We have see in Example 2.3.7 that $\alpha\mathcal{O}_K = PQ_1$ with $P = 2\mathcal{O}_K + (1+\sqrt{-5})\mathcal{O}_K$ and $Q_1 = 3\mathcal{O}_K + (1+\sqrt{-5})\mathcal{O}_K$. This means that $|\alpha|_{P'} = 1$ for all non-zero prime ideals $P' \neq P, Q_1$. Now, note that $P \cap \mathbb{Z} = 2\mathbb{Z}$ and $Q_1 \cap \mathbb{Z} = 3\mathbb{Z}$ and recall that $2\mathcal{O}_K = P^2$ and $3\mathcal{O}_K = Q_1Q_2$. Therefore $e(P) = 2$ and $e(Q_1) = 1$. We conclude that $|\alpha|_P = 2^{-1/2}$ and $|\alpha|_{Q_1} = 3^{-1}$.

Exercise 2.5.12. Let K be a number field. Two absolute values $|\cdot|$ and $\|\cdot\|$ are called **equivalent** if there exists a $\lambda \in (0,\infty)$ such that $|x| = \|x\|^\lambda$ for all $x \in K$.

(i) Let $\sigma : K \to \mathbb{C}$ be an embedding and P a prime ideal of $\mathcal{O}_K$. Show that $|\cdot|_\sigma$ and $|\cdot|_P$ are not equivalent.

(ii) Let P and Q two non-zero prime ideals of $\mathcal{O}_K$, such that $|\cdot|_P$ and $|\cdot|_Q$ are equivalent. Show that $P = Q$.

(iii) Let $\sigma_1, \sigma_2 : K \to \mathbb{C}$ be embeddings such that $|\cdot|_{\sigma_1}$ and $|\cdot|_{\sigma_2}$ are equivalent. Show that $\sigma_1 = \sigma_2$ or that $\sigma_1 = \bar{\sigma}_2$, where $\bar{\cdot}$ denotes complex conjugation.

Recall (Theorem 2.1.5) that, if $d = [K : \mathbb{Q}]$, there are d pairwise distinct embeddings

$$\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}.$$

It is useful to reorder them in the following way.
First, there is an $r \in \mathbb{Z}$ with $0 \leq r \leq d$ such that (after a permutation of the σ_i)

$$\sigma_i(K) \subseteq \mathbb{R} \quad \text{for} \quad 1 \leq i \leq r \quad \text{and} \quad \sigma_i(K) \not\subseteq \mathbb{R} \quad \text{for} \quad r+1 \leq i \leq d.$$

The embeddings $\sigma_1, \ldots, \sigma_r$ are called **real embeddings** of K. For $i > r$ the σ_i are called **complex embeddings** of K. In this case $x \mapsto \overline{\sigma_i}(x) = \overline{\sigma_i(x)}$ is another embedding different from σ_i where $\bar{\cdot}$ denotes complex conjugation. After renumbering again, we can assume

$$\overline{\sigma_{r+1}} = \sigma_{r+s+1},\ \overline{\sigma_{r+2}} = \sigma_{r+s+2},\ \ldots\ , \overline{\sigma_{r+s}} = \sigma_{r+2s}$$

for $s = (d-r)/2$.

Definition 2.5.13. The pair (r, s) that we have associated to the number field K is called the **signature** of K. The number r is the number of real embedddings of K and s the number of pairs of conjugate complex embeddings.

Definition 2.5.14. Let K be a number field. The set $M^0(K)$ of **finite** or **non-archimedean places** of K is

$$M^0(K) = \{P : 0 \neq P \subseteq \mathcal{O}_K \text{ a prime ideal}\}$$

and we identify its elements with the absolute value $|\cdot|_P$ from Definition 2.5.7. We moreover define the set

$$M^\infty(K) = \{\sigma : K \to \mathbb{C} \text{ field embeddings up to conjugation}\}$$

(recall Remark 2.5.9), again identify its element with the corresponding archimedean absolute values of K and call them **archimedean** or **infinite places**. The set of **places** of K is the union $M(K) = M^0(K) \cup M^\infty(K)$.

Remark 2.5.15. Let (r, s) be the signature of K. Then we have

$$\#M^\infty(K) = r + s.$$

In general we write $|\cdot|_v$ for the absolute value that corresponds to $v \in M(K)$.

Lemma 2.5.16. *Let K be a number field and $x \in K^\times = K \setminus \{0\}$. There are at most finitely many $v \in M(K)$ with $|x|_v \neq 1$.*

Proof. We have just seen in Remark 2.5.15 that $M^\infty(K)$ is finite. Therefore, it is enough to show the claim for $M^0(K)$ in place of $M(K)$.
Let $a, b \in \mathcal{O}_K$ be such that $x = a/b$. Then, $|x|_v \neq 1$ implies that $|a|_v \neq 1$ or $|b|_v \neq 1$. But the prime ideal factorization of the ideals $a\mathcal{O}_K$ and $b\mathcal{O}_K$ contain at most finitely many prime ideal. Only for the places corresponding to these prime ideals we may have $|a|_v \neq 1$ or $|b|_v \neq 1$. The lemma follows. □

Definition 2.5.17. For every place v of a number field K we define its **local degree** d_v to be

$$d_v = \begin{cases} 1, & \text{if } v \text{ corresponds to } \sigma : K \to \mathbb{C} \text{ and } \sigma(K) \subseteq \mathbb{R}, \\ 2, & \text{if } v \text{ corresponds to } \sigma : K \to \mathbb{C} \text{ and } \sigma(K) \not\subseteq \mathbb{R}, \\ e(P)f(P), & \text{if } v \text{ corresponds to the prime ideal } P. \end{cases}$$

We now come to an important equality, the so-called product formula. Let us see it first for $\mathbb{Q}$. If p is a prime number and $x \in \mathbb{Q} \setminus \{0\}$ with prime factorization $\pm p_1^{e_1} \cdots p_g^{e_g}$ for some $e_1, \ldots, e_g \in \mathbb{Z}$, we have

$$|x|_p = \begin{cases} 1 & : p \notin \{p_1, \ldots, p_g\} \\ p_i^{-e_i} & : p = p_i. \end{cases}$$

Therefore we have

$$|x| = \prod_p |x|_p^{-1}$$

where the product runs over all prime numbers, but it is actually a finite product as all but at most finitely many factors are different from 1.
We then have

$$|x| \prod_p |x|_p = \prod_{v \in M(\mathbb{Q})} |x|_v = 1$$

for all rational numbers $x \neq 0$.
This is the product formula for rational numbers. We are going to extend this to number fields.

Proposition 2.5.18 (Product formula)**.** *Let K be a number field and $x \in K \setminus \{0\}$. We have*

$$\prod_{v \in M(K)} |x|_v^{d_v} = 1.$$

Proof. We first note that, by the multipicativity of absolute values and by the fact that K is the field of fractions of $\mathcal{O}_K$ it is sufficient to prove the assertion for $x \in \mathcal{O}_K$. We factor the principal ideal $x\mathcal{O}_K$ as $P_1^{e_1} \cdots P_g^{e_g}$, where $e_i \in \mathbb{N}$ and the $P_1, \ldots, P_g$ are pairwise distinct prime ideals of $\mathcal{O}_K$. By definition $\nu_{P_i}(x) = e_i$ and therefore $|x|_{P_i} = {p_i}^{-e_i/e(P_i)}$, where the each p_i is the uniquely determined prime number that lies in P_i.
We now compute the norm of $x\mathcal{O}_K$ and use the multiplicativity of the norm (Proposition 2.4.8) and get

$$N(x\mathcal{O}_K) = N(P_1)^{e_1} \cdots N(P_g)^{e_g} = \prod_{i=1}^{g} p_i^{e_i f(P_i)} = \prod_{i=1}^{g} |x|_{P_i}^{-e(P_i)f(P_i)} = \prod_{i=1}^{g} |x|_{P_i}^{-d_{P_i}}.$$

For all non-zero prime ideals $P \notin \{P_1, \ldots, P_g\}$ we have $|x|_P = 1$, and thus

$$N(x\mathcal{O}_K) = \prod_{P \in M^0(K)} |x|_P^{-d_P}. \tag{2.9}$$

On the other hand, Lemma 2.4.5(iv) gives $N(x\mathcal{O}_K) = \prod_{\sigma: K \to \mathbb{C}} |\sigma(x)|$. We combine this with (2.9) and obtain

$$\prod_{P \in M^0(K)} |x|_P^{-d_P} = \prod_{v \in M^\infty(K)} |x|_v^{d_v}$$

which was what we had to show. □

Exercise 2.5.19 (Gauss' Lemma)**.** Let $P \in M^0(K)$ be a finite place of K, that is, a non-zero prime ideal of $\mathcal{O}_K$. Given a polynomial $b_0 X^m + \cdots + b_m \in K[X]$ we set

$$|b_0 X^m + \cdots + b_m|_P = \max\{|b_0|_P, \ldots, |b_m|_P\}$$

Prove that $|BC|_P = |B|_P |C|_P$ for all $B, C \in K[X]$.

3 The Weil height

We give two definition of height and we are going to see that they are equivalent. Both definitions have their pros and cons.

3.1 The height via Mahler measure

The first definition of height comes from the minimal polynomial and takes the form of Definition 1.1.1 in the rational case.

Definition 3.1.1. Let $P = a_0X^d + \cdots + a_d = a_0(X - x_1)\cdots(X - x_d)$ be a non-zero complex polynomial. We define the **Mahler measure** of P to be

$$M(P) = |a_0| \prod_{i=1}^{d} \max\{1, |x_i|\}$$

and we set $M(0) = 0$.

Definition 3.1.2 (Height - First definition)**.** Let x be an algebraic number. After multiplying its minimal polynomial over $\mathbb{Q}$ with an appropriate integer we get a uniquely determined poynomial $P = a_0X^d + \cdots + a_d \in \mathbb{Z}[X] \setminus \{0\}$ such that

(i) $P(x) = 0$,
(ii) P is irreducible in $\mathbb{Q}[X]$.
(iii) the coefficients $a_0, \ldots, a_d$ do not have any common prime divisor and $a_0 \geq 1$.

Over $\mathbb{C}$ we have the factorization $P = a_0(X - x_1)\cdots(X - x_d)$, where $x_1, \ldots, x_d \in \mathbb{C}$. We define the **Weil height** of x to be

$$h(x) = \frac{1}{d}\log M(P) = \frac{1}{d}\log\left(a_0 \prod_{i=1}^{d} \max\{1, |x_i|\}\right).$$

Example 3.1.3.

(i) Let $x = a/b$ be a rational number with $a, b \in \mathbb{Z}$ coprime and and $b \geq 1$. The polynomial P from the above definition is $P = bX - a$. We have $d = 1$ and $x_1 = x$, therefore $h(x) = \log(b\max\{1, |x|\}) = \log\max\{|a|, b\}$. Therefore this definition generalizes Definition 1.1.1.

(ii) Let $x = 2^{1/d}$ and $d \geq 1$. Then $P = X^d - 2$ is irreducible because of Eisenstein Criterion with respect to the prime number $p = 2$. The complex roots of P are

$$2^{1/d}e^{2\pi ia/d} \quad \text{for} \quad a \in \{0, \ldots, d-1\}$$

and they all have absolute value $2^{1/d}$ and P satisfies the three conditions of Definition 3.1.2 for $x = 2^{1/d}e^{2\pi ia/d}$. It follows that $h(2^{1/d}e^{2\pi ia/d}) = (\log 2)/d$.

(iii) Set $x = 1 + \sqrt{2}$. Then $P = X^2 - 2X - 1$ is the minimal polynomial of x and it satisfies the conditions we need. Its complex roots are $x_1 = 1+\sqrt{2}$ and $x_2 = 1-\sqrt{2}$. We get

$$h(1 \pm \sqrt{2}) = \frac{1}{2}\log(1 + \sqrt{2}).$$

Exercise 3.1.4. Let K be a number field and $x \in K \setminus \{0\}$. Show that $h(x) = h(\pm 1/x)$

Remark 3.1.5. Note that, if $x \in \mathcal{O}_K$, the polynomial P of the above definition is actually the minimal polynomial of x and therefore

$$h(x) = \frac{1}{d}\log\left(\prod_{i=1}^{d}\max\{1, |x_i|\}\right).$$

Exercise 3.1.6. Let $m < 0$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{m})$. Let $x \in \mathcal{O}_K \setminus \{0\}$. Show that $h(x) = \frac{1}{2}\log N_{K/\mathbb{Q}}(x)$.

Exercise 3.1.7. Calculate the height of

$$1 + \sqrt{5} + \sqrt{2020}, \quad 1 + e^{2\pi i/5}, \quad \frac{\sqrt{2}}{2}.$$

3.2 The height via absolute values

We now give another definition of height. We are going to see later that it is equivalent to the one given in Definition 3.1.2.

Definition 3.2.1 (Height - Second definition)**.** Let K be a number field and $x \in K$. We define the **Weil height** of x with respect to K to be $h_K(x) = h_K^0(x) + h_K^\infty(x)$ where

$$h_K^0(x) = \frac{1}{[K:\mathbb{Q}]}\sum_{P \in M^0(K)} e(P)f(P)\log\max\{1, |x|_P\} \tag{3.1}$$

and

$$h_K^\infty(x) = \frac{1}{[K:\mathbb{Q}]}\sum_{v \in M^\infty(K)} d_v \log\max\{1, |x|_v\}. \tag{3.2}$$

We recall that every $v \in M^\infty(K)$ corresponds to $|\cdot|_\sigma$ for an embedding $\sigma : K \to \mathbb{C}$ that is uniquely determined modulo complex conjugation and we set

$$d_v = \begin{cases} 1 & \text{if } \sigma(K) \subseteq \mathbb{R} \\ 2 & \text{if } \sigma(K) \not\subseteq \mathbb{R}. \end{cases} \tag{3.3}$$

Moreover, $e(P)$ is the ramification index of P and $f(P)$ the residue degree of P, i.e. the norm $N(P)$ of P satisfies $\#\mathcal{O}_K/P = N(P) = p^{f(P)}$. We often write $d_P = e(P)f(P)$.

Remark 3.2.2. (i) For the "infinite" part of the height, i.e., the sum $h_K^\infty(x)$ over $M^\infty(K)$ in (3.2), we have

$$\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M^\infty(K)} d_v \log\max\{1,|x|_v\} = \frac{1}{[K:\mathbb{Q}]}\sum_{\sigma:K\to\mathbb{C}} \log\max\{1,|\sigma(x)|\}, \tag{3.4}$$

because a complex embedding and its conjugate give two equal terms in the sum on the right hand side. This explain the factor d_v in the definition.

(ii) In the notation of the definition and for all $P \in M^0(K)$, the factors $e(P)f(P)$ are normalizing constants that come from the product formula.

(iii) We are going to prove later that $h_K(x)$ from Definition 3.2.1 is equal to $h(x)$ from Definition 3.1.2. In particular, $h_K(x)$ is independent of K, meaning that, if $F \subset K$ is a subfield and $x \in F$, then $h_F(x) = h_K(x)$.

Example 3.2.3. Let $d \geq 1$ be an integer and $x = 2^{1/d}$ with minimal polynomial $X^d - 2$ over $\mathbb{Q}$ as in Example 3.1.3(ii). In particular x is an algebraic integer. Let K be a number field containing x. Thus, $x \in \mathcal{O}_K$. We determine $|x|_v$ for all $v \in M(K)$.
If $v \in M^0(K)$, then $v = P$ is a non-zero prime ideal of $\mathcal{O}_K$. As, $x \in \mathcal{O}_K$ we have $\nu_P(x) \geq 0$. It follows $|x|_v \leq 1$ and thus $\log\max\{1,|x|_v\} = \log 1 = 0$ and v does not give any contribution to $h_K(x)$.
If $v \in M^\infty(K)$, there is a field embedding $\sigma : K \to \mathbb{C}$ with $|x|_v = |\sigma(x)|$. Since $\sigma(x)^d = \sigma(x^d) = \sigma(2) = 2$ we have

$$|x|_v = |\sigma(x)| = 2^{1/d}.$$

and thus $\log\max\{1,|x|_v\} = (\log 2)/d$.
By Definition 3.2.1 we have

$$h_K(x) = \frac{\log 2}{d}\frac{1}{[K:\mathbb{Q}]}\sum_{v\in M^\infty(K)} d_v.$$

Finally, we have that $\sum_{v\in M^\infty(K)} d_v = \sum_{\sigma:K\to\mathbb{C}} 1 = [K:\mathbb{Q}]$.
We have just verified that our two definition of height coincide for $2^{1/d}$.

We now prove that $h_K(x)$ is independent of K.

Lemma 3.2.4. *Let K be a number field and F/K a finite field extension. For all $x \in K$ we have*

$$h_K^0(x) = h_F^0(x) \quad \text{and} \quad h_K^\infty(x) = h_F^\infty(x) \tag{3.5}$$

and therefore $h_K(x) = h_F(x)$.

Proof. For all prime ideals $P \neq 0$ of $\mathcal{O}_K$ we have that $P\mathcal{O}_F$ is an ideal of $\mathcal{O}_F$ (not necessarely prime). We know it factors

$$P\mathcal{O}_F = \mathfrak{P}_1^{e(P,1)} \cdots \mathfrak{P}_{g(P)}^{e(P,g(P))}, \tag{3.6}$$

where $\mathfrak{P}_i$ are prime ideals of $\mathcal{O}_F$.
We now calculate the norm of $P\mathcal{O}_F$ with the help of Proposition 2.4.8 and Lemma 2.4.10. We have

$$\begin{aligned} p^{f(P)[F:K]} &= N(P)^{[F:K]} = N(P\mathcal{O}_F) = N(\mathfrak{P}_1)^{e(P,1)} \cdots N(\mathfrak{P}_{g(P)})^{e(P,g(P))} \\ &= p^{f(\mathfrak{P}_1)e(P,1)+\cdots+f(\mathfrak{P}_{g(P)})e(P,g(P))}, \end{aligned}$$

where p is the prime number that lies in P, and therefore in all the $\mathfrak{P}_i$. Comparing exponents we have

$$f(P)[F:K] = f(\mathfrak{P}_1)e(P,1) + \cdots + f(\mathfrak{P}_{g(P)})e(P,g(P)), \tag{3.7}$$

and we are going to use this identity later.
We may suppose $x \neq 0$. Let (for the moment) $x \in \mathcal{O}_K$ and let

$$x\mathcal{O}_K = \prod_P P^{\nu_P(x)}$$

be the factorization of the principal ideal generated by x in non-zero prime ideals of $\mathcal{O}_K$. This gives

$$x\mathcal{O}_F = \prod_P (P\mathcal{O}_F)^{\nu_P(x)}.$$

By the factorization (3.6) it follows that $\nu_{\mathfrak{P}_i}(x) = e(P,i)\nu_P(x)$ for prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_F$ containing $P\mathcal{O}_F$. One can easily see that this last equality extends to any $x \in K \setminus \{0\}$, by writing x as a fraction a/b of elements of $\mathcal{O}_K$ and using $\nu(x) = \nu(a) - \nu(b)$ for any valuation ν.
Now we have

$$e(\mathfrak{P}_i)\log|x|_{\mathfrak{P}_i} = \log p^{-\nu_{\mathfrak{P}_i}(x)} = e(P,i)\log p^{-\nu_P(x)} = e(P,i)e(P)\log|x|_P, \tag{3.8}$$

and therefore, using (3.8) and (3.7),

$$\begin{aligned} [F:\mathbb{Q}]h_F^0(x) &= \sum_{\mathfrak{P}\in M^0(F)} e(\mathfrak{P})f(\mathfrak{P})\log\max\{1,|x|_{\mathfrak{P}}\} \\ &= \sum_{P\in M^0(K)} \sum_{i=1}^{g(P)} f(\mathfrak{P}_i)e(P,i)e(P)\log\max\{1,|x|_P\} \\ &= \sum_{P\in M^0(K)} e(P)\log\max\{1,|x|_P\} \sum_{i=1}^{g(P)} f(\mathfrak{P}_i)e(P,i) \\ &= [F:K] \sum_{P\in M^0(K)} e(P)f(P)\log\max\{1,|x|_P\} \\ &= [F:K][K:\mathbb{Q}]h_K^0(x) = [F:\mathbb{Q}]h_K^0(x), \end{aligned}$$

and we are done with the first part of the lemma.

The second equality is simpler. We know that every field embedding $K \to \mathbb{C}$ can be extended in exactly $[F : K]$ distinct ways to a field emebedding $F \to \mathbb{C}$. Recalling (3.4) we have

$$[F : \mathbb{Q}]h_F^\infty(x) = \sum_{\sigma : F \to \mathbb{C}} \log \max\{1, |\sigma(x)|\} = [F : K] \sum_{\sigma : K \to \mathbb{C}} \log \max\{1, |\sigma(x)|\}$$

and the right hand side equals $[F : K][K : \mathbb{Q}]h_K^\infty(x)$. We then have the second equality. □

Remark 3.2.5. The lemma we have just proved justifies the factor $1/[K : \mathbb{Q}]$ in Definition 3.2.1.

We see now an important property of the height.

Lemma 3.2.6. *Let K, F be two number fields and $\varphi : K \to F$ a non-zero ring homomorphism. Then we have $h_K(x) = h_F(\varphi(x))$ for all $x \in K$. Actually, we have $h_K^0(x) = h_F^0(\varphi(x))$ and $h_K^\infty(x) = h_F^\infty(\varphi(x))$.*

Proof. As φ is injective and by Lemma 3.2.4 we are allowed to replace F by $\varphi(K)$, we may assume that φ is an isomorphism.
Now it is easy to see that, if P is a prime ideal of $\mathcal{O}_F$, then $\varphi^{-1}(P)$ is a prime ideal of $\mathcal{O}_K$. Moreover, we have $N(P) = N(\varphi^{-1}(P))$, thus $f(P) = f(\varphi^{-1}(P))$. Let p be the uniquely determined prime number in P. The equality $e(P) = e(\varphi^{-1}(P))$ is obvious by comparing the factorizations of $p\mathcal{O}_K$ and $p\mathcal{O}_F$.
On the other hand, for a field embedding $\sigma : F \to \mathbb{C}$ we have that $\sigma \circ \varphi : K \to \mathbb{C}$ is a field embedding.
Therefore, we associate to every element $v \in M(F)$ an element $w = \varphi^* v \in M(K)$. It is clear that, for all $x \in K$ and $v \in M(F)$, $|x|_{\varphi^* v} = |\varphi(x)|_v$ and thus

$$\begin{aligned} h_F(\varphi(x)) &= \frac{1}{[F : \mathbb{Q}]} \sum_{v \in M(F)} d_v \log \max\{1, |\varphi(x)|_v\} \\ &= \frac{1}{[K : \mathbb{Q}]} \sum_{w \in M(K)} d_w \log \max\{1, |x|_w\} = h_K(x). \end{aligned}$$

The same equalities hold if we consider only places in $M^0(F)$ or $M^\infty(F)$ in the sum. □

The following lemma will help us proving that the two definitions of height we have seen are equivalent.

Lemma 3.2.7. *Let K be a number field and $x \in K$. Let $A \in \mathbb{Z}[X]$ be the uniquely determined polynomial with $A(x) = 0$, that is irreducible in $\mathbb{Q}[X]$ and has coprime coefficients and leading coefficient $a_0 \geq 1$. We have*

$$\frac{\log a_0}{[\mathbb{Q}(x) : \mathbb{Q}]} = h_K^0(x). \tag{3.9}$$

Proof. By Lemma 3.2.4 we may replace K by a larger number field.
Therefore, we may assume that A splits in linear factors over K and thus $A = a_0(X - x_1)\cdots(X - x_d)$ with $x_1, \dots, x_d \in K$.
Let $P \in M^0(K)$ be a finite place of K, that is, a non-zero prime ideal of $\mathcal{O}_K$. Recall Exercise 2.5.19. Given a polynomial $b_0X^m + \cdots + b_m \in K[X]$ we set

$$|b_0X^m + \cdots + b_m|_P = \max\{|b_0|_P, \dots, |b_m|_P\}$$

We have $|BC|_P = |B|_P|C|_P$ for all $B, C \in K[X]$.
Since the coefficients of A do not have any common prime divisor we have $|A|_P = 1$. Therefore

$$1 = |A|_P = |a_0|_P|X - x_1|_P \cdots |X - x_d|_P = |a_0|_P \max\{1, |x_1|_P\} \cdots \max\{1, |x_d|_P\}.$$

Recall that $P \in M^0(K)$ was arbitrary. From this we get

$$\prod_{P\in M^0(K)} |a_0|_P^{-d_P} = \prod_{P\in M^0(K)} \prod_{i=1}^{d} \max\{1, |x_i|_P\}^{d_P} = \prod_{i=1}^{d} \prod_{P\in M^0(K)} \max\{1, |x_i|_P\}^{d_P}.$$

By the product formula (Proposition 2.5.18), we can express the left hand side as a product over the infinite places of K. Recalling that we have $\sum_{v\in M^\infty(K)} d_v = r + 2s = [K : \mathbb{Q}]$, where (r, s) is the signature of K, we obtain

$$\prod_{i=1}^{d} \prod_{P\in M^0(K)} \max\{1, |x_i|_P\}^{d_P} = \prod_{v\in M^\infty(K)} |a_0|_v^{d_v} = a_0^{\sum_{v\in M^\infty(K)} d_v} = a_0^{[K:\mathbb{Q}]}.$$

Taking logarithms we have

$$\sum_{i=1}^{d} \underbrace{\sum_{P\in M^0(K)} d_P \log \max\{1, |x_i|_P\}}_{=[K:\mathbb{Q}]h_K^0(x_i)} = [K : \mathbb{Q}] \log a_0. \tag{3.10}$$

Now, by Lemma 3.2.4 we have $h_K^0(x_i) = h_{\mathbb{Q}(x_i)}^0(x_i)$ and we know that for all i there is an isomorphism $\mathbb{Q}(x) \to \mathbb{Q}(x_i)$, that sends x to x_i. Lemma 3.2.6 implies that $h_{\mathbb{Q}(x_i)}(x_i) = h_{\mathbb{Q}(x)}(x)$.
Using (3.10) we have $d[K : \mathbb{Q}]h_{\mathbb{Q}(x)}^0(x) = [K : \mathbb{Q}] \log a_0$ and we obtain (3.9) because $d = [\mathbb{Q}(x) : \mathbb{Q}]$ and $h_{\mathbb{Q}(x)}^0(x) = h_K^0(x)$. □

Finally, we can prove the following theorem.

Theorem 3.2.8. *Let K be a number field and $x \in K$. Then, $h_K(x) = h(x)$. In other words, the two definitions 3.1.2 and 3.2.1 of Weil height coincide.*

Proof. By Lemma 3.2.4 we may assume that $K = \mathbb{Q}(x)$. Let A be the polynomial from the statement of Lemma 3.2.7. By Definition 3.1.2 and using (3.9), we have

$$h(x) = h^0_{\mathbb{Q}(x)}(x) + \frac{1}{[\mathbb{Q}(x) : \mathbb{Q}]} \sum_{i=1}^{d} \max\{1, \log |z_i|\}$$

where $z_1, \ldots, z_d$ are the complex roots of A. But the z_i are exactly the $\sigma(x)$ for σ running through the field embeddings $K \to \mathbb{C}$. The desired equality now follows from (3.4). □

Example 3.2.9. Let x be the only real number such that $x^3 = x + 1$. Then, x is an algebraic integer and therefore $h^0_K(x) = 0$. The only contribution to the height comes form the infinite places. There are three embeddings $\sigma_{1,2,3} : \mathbb{Q}(x) \to \mathbb{C}$, where σ_1 is real and $\sigma_{2,3}$ are a pair of complex conjugate embeddings. We have

$$1 = \sigma_1(x)\sigma_2(x)\sigma_3(x) = |x||\sigma_2(x)|^2$$

As $x > 1$ it follows that $|\sigma_2(x)| < 1$. The number x is an example of **Pisot number**, i.e., x is a real algebraic integer greater than 1 all of whose images via the other embeddings in $\mathbb{C}$ are less than 1 in absolute value. Siegel proved that x is the smallest Pisot number. This $x > 1$ is called **Plastic number**. It follows that

$$h(x) = \frac{1}{3} \log x.$$

By Cardano's formula we have

$$x = \frac{1}{6} \left((108 + 12\sqrt{69})^{1/3} + (108 - 12\sqrt{69})^{1/3} \right).$$

Therefore,

$$h(x) = 0.09373319144098728217 \ldots. \tag{3.11}$$

Exercise 3.2.10. Calculate the height of

$$\alpha = \frac{2 + \sqrt{-5}}{2 - \sqrt{-5}}$$

using the two definitions of height.

Exercise 3.2.11. We define the height of a point $x = [x_0 : \cdots : x_n]$ of the projective space $\mathbb{P}^n(\overline{\mathbb{Q}})$ to be

$$h([x_0 : \cdots : x_n]) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M(K)} d_v \log \max\{|x_0|_v, \ldots, |x_n|_v\},$$

where K is any number field containing $x_0, \ldots, x_n$. Prove that it is well defined and independent of the choice of K.

3.3 Properties of the Weil height

In Lemma 1.1.4 we have seen that the height of rational numbers satisfies nice properties when we consider powers and products. Here we prove the same properties for the Weil height.

Lemma 3.3.1. *Let x be an algebraic number.*
(i) If $x \neq 0$ and if $k \geq 0$ is an integer, it follows that $h(x^k) = kh(x)$.
(ii) If y is an algebraic number we have that $h(xy) \leq h(x) + h(y)$.

Proof. For both claims we use the second definition of height. For part (i) we note that

$$\max\{1, s^k\} = \max\{1, s\}^k$$

for all $s > 0$. For all places v of a number field K with $x \in K$ we have $\max\{1, |x^k|_v\} = \max\{1, |x|_v^k\} = \max\{1, |x|_v\}^k$. We take logarithms and multiply by d_v, sum over all v, divide by $[K : \mathbb{Q}]$ and obtain

$$h(x^k) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M(K)} d_v \log(\max\{1, |x|_v\}^k) = kh(x),$$

and this is what we had to show.
Part (ii) follows analogously with the help of the following simple fact

$$\max\{1, st\} \leq \max\{1, s\} \max\{1, t\},$$

for all real numbers $s, t \geq 0$. □

Example 3.3.2. We already know that $h(0) = h(\pm 1) = 0$. But there are more algebraic numbers with height zero. Let ζ be a root of unity, meaning $\zeta^n = 1$ for some positive integer n. We have

$$0 = h(1) = h(\zeta^n) = nh(\zeta).$$

Therefore $h(\zeta) = 0$.
Which other algebraic numbers have height zero? Here and for the course we fix an algebraic closure $\overline{\mathbb{Q}}$ of the rational numbers.
Let

$$S = \{x \in \overline{\mathbb{Q}}^\times \text{ with } h(x) = 0\}. \tag{3.12}$$

For $x, y \in S$ we have, by Lemma 3.3.1, $h(xy) \leq h(x) + h(y) = 0$, and therefore $xy \in S$, since the height cannot be negative. Therefore the set S is closed under multiplication.

We now use the product formula to show that the height is invariant under taking inverses.

Lemma 3.3.3. *Let $x \neq 0$ be an algebraic number. Then, we have $h(x) = h(x^{-1})$. Moreover, $h(x^k) = |k|h(x)$ for all $k \in \mathbb{Z}$.*

Proof. The second claim follows from the first together with Lemma 3.3.1(i).
By definition we have

$$[\mathbb{Q}(x):\mathbb{Q}]h(x^{-1}) = \sum_{P\in M^0(K)} e(P)f(P)\log\max\{1,|x|_P^{-1}\} + \sum_{\sigma:K\to\mathbb{C}} \max\{1,|x|_\sigma^{-1}\}.$$

We add

$$0 = \sum_{P\in M^0(K)} e(P)f(P)\log|x|_P + \sum_{\sigma:K\to\mathbb{C}} \log|x|_\sigma,$$

which is obtained form the product formula (Proposition 2.5.18). We obtain the claim noting that

$$\log\max\{1,t^{-1}\} + \log t = \log\max\{1,t\}$$

for all $t>0$. □

Example 3.3.4. We deduce that the set S defined in (3.12) is a subgroup of the multiplicative group of all algebraic numbers.

Exercise 3.3.5. Let $\alpha,\beta\in\overline{\mathbb{Q}}\setminus\{0\}$. Prove that $h(\alpha\beta)\geq|h(\alpha)-h(\beta)|$.

We can also bound the Weil height of a sum as we did for the product.

Lemma 3.3.6. *For $x,y\in\overline{\mathbb{Q}}$ we have $h(x+y)\leq h(x)+h(y)+\log 2$.*

Proof. Let $K=\mathbb{Q}(x,y)$ and $v\in M(K)$.
If $v=P\in M^0(K)$, we have $|x+y|_P\leq\max\{|x|_P,|y|_P\}$ and therefore

$$\max\{1,|x+y|_P\}\leq\max\{1,|x|_P\}\max\{1,|y|_P\}.$$

If $v\in M^\infty(P)$ we use

$$\max\{1,|x+y|_v\}\leq\max\{1,|x|_v+|y|_v\}\leq 2\max\{1,|x|_v\}\max\{1,|y|_v\}. \tag{3.13}$$

Finally, we combine this and obtain

$$\begin{aligned}[K:\mathbb{Q}]h(x+y) &= \sum_{P\in M^0(K)} e(P)f(P)\log\max\{1,|x+y|_P\} + \sum_{\sigma:K\to\mathbb{C}}\log\max\{1,|x+y|_\sigma\}\\ &\leq [K:\mathbb{Q}](h(x)+h(y)+\log 2),\end{aligned}$$

where $\log 2$ comes for the factor 2 in (3.13). □

Remark 3.3.7. It is easy to see that the above lemma can be generalized to sums of an arbitrary number of algebraic numbers. Indeed, for all $x_1,\dots,x_n\in\overline{\mathbb{Q}}$, we have

$$h(x_1+\cdots+x_n)\leq\sum_{i=1}^n h(x_i)+\log n.$$

Exercise 3.3.8. Let $\alpha, a_1, \dots, a_d \in \overline{\mathbb{Q}}$ with the a_i not all zero, be such that $\alpha^d + a_1\alpha^{d-1} + \cdots + a_d = 0$. Show that

$$h(\alpha) \leq \sum_{i=1}^{d} h(a_i) + \log d.$$

Exercise 3.3.9. Recall we have defined the height in projective space in Exercise 3.2.11. Prove that, for all $x_1, \dots, x_n \in \overline{\mathbb{Q}}$ we have

$$\max\{h(x_1), \dots, h(x_n)\} \leq h([1 : x_1 : \cdots : x_n]).$$

Next, we are going to see the analogues of properties (i) and (vi) in Lemma 1.1.4.

Remark 3.3.10. The finiteness property (vi) in Lemma 1.1.4 cannot be directly translated to algebraic numbers. Indeed, the set

$$\{x \in \overline{\mathbb{Q}} : h(x) \leq 1\} \tag{3.14}$$

contains, in addition to 0, all roots of unity, see Example 3.3.2. In particular, the set defined in (3.14) is infinite. It also contains all $2^{1/d}$ with $d \geq 1$, recall Example 3.2.3.

We note that the elements of (3.14) we have exhibited have degree over $\mathbb{Q}$ that tends to infinity. There is a replacement for the finiteness result in Lemma 1.1.4(vi). One needs to bound the degree in addition to the Weil height.

Theorem 3.3.11 (Northcott)**.** *Let B and D be real numbers. Then*

$$\left\{x \in \overline{\mathbb{Q}} : h(x) \leq B \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] \leq D\right\}$$

is a finite set.

Proof. For the proof of Northcott's Theorem we use the defition of the height via the Mahler measure.
Let $x \in \overline{\mathbb{Q}}$ with $h(x) \leq B$ and $[K : \mathbb{Q}] \leq D$ with $K = \mathbb{Q}(x)$. Let moreover $A \in \mathbb{Z}[X]$ with $A(x) = 0$, A irreducible in $\mathbb{Q}[X]$ with coprime coefficients and leading $a_0 \geq 1$. Over $\mathbb{C}$ the polynomial A splits in linear factors $A = a_0(X - x_1)\cdots(X - x_d)$.
The Mahler measure of A satisfies

$$M(A) = a_0 \prod_{i=1}^{d} \max\{1, |x_i|\} = e^{\deg(A)h(x)} = e^{[\mathbb{Q}(x):\mathbb{Q}]h(x)} \leq e^{DB}.$$

We immediately have $1 \leq a_0 \leq e^{DB}$.
Let $A = a_0X^d + a_1X^{d-1} + \cdots + a_d$ with $a_1, \dots, a_d \in \mathbb{Z}$.
We now use the fact that the coefficients of A/a_0 can be expressed as elementary symmetric polynomials in the roots of A. We get

$$|a_1| = a_0|x_1 + \cdots + x_d| \leq da_0 \max\{1, |x_1|\}\cdots\max\{1, |x_d|\} \leq de^{DB} \leq De^{DB}$$
$$|a_2| = a_0\left|\sum_{i<j} x_ix_j\right| \leq \binom{d}{2} a_0 \max\{1, |x_1|\}\cdots\max\{1, |x_d|\} \leq \binom{d}{2} e^{DB}.$$

For a general $k \in \{1, \dots, d\}$ we have

$$|a_k| = a_0 \left| \sum_{i_1 < \cdots < i_k} x_{i_1} \cdots x_{i_k} \right| \leq a_0 \max\{1, |x_1|\} \cdots \max\{1, |x_d|\} \sum_{i_1 < \cdots < i_k} 1$$
$$= \binom{d}{k} e^{[\mathbb{Q}(x):\mathbb{Q}]h(x)} \leq \binom{d}{k} e^{DB}.$$

Since $\binom{d}{k} \leq 2^d \leq 2^D$ we get

$$|a_k| \leq e^{DB} 2^D \quad \text{for all} \quad k \in \{0, \dots, d\}. \tag{3.15}$$

The coefficients of A are therefore bounded in term of B and D. Since $d \leq D$, there are at most finitely many possibilities for $a_0, \dots, a_d$ and the same for A. Now a degree d polynomial has at most d distinct roots and we have at most finitely many possibilities for x, which was what we had to show. □

Exercise 3.3.12. Prove Northcott's Theorem for the projective space $\mathbb{P}^n(\overline{\mathbb{Q}})$, namely, for all B and D be real numbers we have that

$$\big\{x \in \mathbb{P}^n(\overline{\mathbb{Q}}) : h(x) \leq B \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] \leq D\big\}$$

is a finite set.
Here by $\mathbb{Q}(x)$ we mean the field of definition of $x = [x_0 : \cdots : x_n]$, i.e.,

$$\mathbb{Q}\left(\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}\right) \quad \text{for any } x_i \neq 0.$$

Exercise 3.3.13. Let $x \in \overline{\mathbb{Q}}$ and $A = a_0 X^d + \cdots + a_d \in \mathbb{Z}[X]$ the polynomial from the proof above. Let $D \geq 1$. We have proved that $|a_k| \leq e^{DB} 2^D$ for all $0 \leq k \leq d$, if $h(\alpha) \leq B$ and $[\mathbb{Q}(x) : \mathbb{Q}] \leq D$.

(i) Show that

$$\#\big\{\alpha \in \overline{\mathbb{Q}} : h(\alpha) \leq (\log 2)/D \text{ and } [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq D\big\} \leq D(2^{D+2}+1)^{D+1} \leq 2^{(D+1)(D+3)}.$$

(ii) Let $h(\alpha) > 0$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq D$, show that

$$h(\alpha) > 2^{-(D+1)(D+3)} \frac{\log 2}{D}.$$

Hint: $1, \alpha, \alpha^2, \alpha^3, \dots$ and (i).

The so called Northcott's Theorem has many applications in number theory. We immediately use it to extend Lemma 1.1.4(i). We have seen in Example 3.3.2, that 0 and all roots of unity have height zero. Kronecker's Theorem shows the converse.

Theorem 3.3.14 (Kronecker)**.** *Let ζ be an algebraic number with $h(\zeta) = 0$. Then $\zeta = 0$ or ζ is a root of unity.*

Proof. As $h(\zeta) = 0$ it follows from Lemma 3.3.1(i) that

$$h(\zeta) = h(\zeta^2) = h(\zeta^3) = \cdots = 0.$$

But the powers ζ^k with $k \geq 0$ lie in the number field $K = \mathbb{Q}(\zeta)$ and therefore in

$$\{x \in \overline{\mathbb{Q}} : h(x) = 0 \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] \leq [\mathbb{Q}(\zeta) : \mathbb{Q}]\}.$$

This set is finite by Northcott's Theorem and contains the sequence $\zeta, \zeta^2, \zeta^3, \ldots$. Therefore there exist $k < l$ in $\mathbb{N}$ with $\zeta^k = \zeta^l$.
If $\zeta \neq 0$, then $\zeta^{l-k} = 1$ and we have showed that ζ is a root of unity. □

Remark 3.3.15. Kronecker's original statement was not formulated in terms of heights and read: if all the conjugates of an algebraic integer $\alpha \neq 0$ have absolute value ≤ 1, then α is a root of unity.

Exercise 3.3.16. Let μ_∞ be the subgroup of $\overline{\mathbb{Q}}^\times$ whose elements are the roots of unity. We consider the quotient $\overline{\mathbb{Q}}^\times/\mu_\infty$.

(i) Prove that, given $\lambda \in \mathbb{Q}$, x^λ is a well defined element of $\overline{\mathbb{Q}}^\times/\mu_\infty$ for all $x \in \overline{\mathbb{Q}}^\times/\mu_\infty$.
(ii) Prove that $\overline{\mathbb{Q}}^\times/\mu_\infty$ with the group operation as addition and $(\lambda, x) \mapsto x^\lambda$ as scalar multiplication is a $\mathbb{Q}$ vector space.
(iii) Show that the Weil height is well-defined for elments of $\overline{\mathbb{Q}}^\times/\mu_\infty$ and gives a norm on this $\mathbb{Q}$-vector space.

3.4 Lehmer's problem

We now discuss the historical origin of the height function. In a work dating back to 1933 Derrick Lehmer was trying to construct prime numbers with the help of polynomials. The approach worked roughly as follows. One begins with a polynomial $A \in \mathbb{Z}[X] \setminus \mathbb{Z}$. Over the complex numbers A splits in linear factors

$$A = (X - x_1) \cdots (X - x_d)$$

with $x_1, \ldots, x_d \in \mathbb{C}$. After substituting 1, we get an integer

$$(x_1 - 1) \cdots (x_d - 1) = \pm A(1).$$

For all $n \geq 1$. we consider the polynomial

$$A_n = (X - x_1^n) \cdots (X - x_d^n).$$

Note that, even if A had distinct roots, this might not be the case anymore for A_n.
A priori A_n has coefficients in $\mathbb{C}$. On the other hand, every coefficient of A_n is a symmetric polynomial in the roots $x_1^n, \ldots, x_d^n$ of A_n and is therefore a symmetric polynomial in the roots $x_1, \ldots, x_d$ of A. The fundamental Theorem of symmetric polynomial implies that the coefficients of A_n can be expressed as polynomials in the coefficients of

A because the latter are elementary symmetric polynomials in $x_1, \dots, x_d$. This forces $A_n \in \mathbb{Z}[X]$.
Lehmer was looking for prime divisors of

$$\Delta_n = \Delta_n(A) = (x_1^n - 1) \cdots (x_d^n - 1) = (-1)^d A_n(1) \quad \text{for increasing} \quad n.$$

Example 3.4.1. (i) First consider the easy case $A = X - 2$. Then, $A_n = X - 2^n$, and thus

$$\Delta_n = -A_n(1) = 2^n - 1.$$

A Mersenne prime number is a prime number of the form $2^n - 1$, which therefore appears in the sequence Δ_n. Most record prime numbers a Mersenne primes. Indeed, the largest known prime number is (at the moment) the Mersenne prime $2^{82.589.933} - 1 = \Delta_{82.589.933}$. It is not known though if there are infinitely many Mersenne primes.

(ii) We consider the minimal polynomial $A = X^3 - X - 1$ of the plastic number from Example 3.2.9. We have

n	A_n	$\Delta_n = (-1)^3 A_n(1)$
1	$X^3 - X - 1$	1
2	$X^3 - 2X^2 + X - 1$	1
3	$X^3 - 3X^2 + 2X - 1$	1
4	$X^3 - 2X^2 - 3X - 1$	5
5	$X^3 - 5X^2 + 4X - 1$	1
6	$X^3 - 5X^2 - 2X - 1$	7
$\vdots$	$\vdots$	$\vdots$
41	$X^3 - 101639X^2 + 532X - 1$	101107
$\vdots$	$\vdots$	$\vdots$
57	$X^3 - 9141872X^2 + 4543X - 1$	$9137329 = 229 \cdot 39901$

Not every value Δ_n is a prime number but nevertheless prime numbers appear sporadically.

By cleverly choosing the polynomial A, Lehmer hoped to find many large prime numbers among the values of Δ_n (and its divisors). An important question is how to find a suitable polynomial A. It turns out that it's especially helpful when the sequence

$$\Delta_1, \Delta_2, \Delta_3, \dots$$

grows as slowly as possible in absolute value.
For the sake of simplicity we assume that $|x_i| \neq 1$ for all $i \in \{1, \dots, d\}$. This condition is fulfilled in the two examples above[1]. We consider

$$\left| \frac{\Delta_{n+1}}{\Delta_n} \right| = \prod_{i=1}^{d} \left| \frac{x_i^{n+1} - 1}{x_i^n - 1} \right|.$$

[1]Many of the following results are also true, if $|x_i| = 1$ for an i. But the proofs are much more difficult.

By hypothesis we have $|x_i| \neq 1$. If $|x_i| > 1$ then

$$\lim_{n\to\infty} \left| \frac{x_i^{n+1} - 1}{x_i^n - 1} \right| = |x_i|$$

while in case $|x_i| < 1$ we have

$$\lim_{n\to\infty} \left| \frac{x_i^{n+1} - 1}{x_i^n - 1} \right| = 1.$$

In both cases the limit exists and is equal $\max\{1, |x_i|\}$. We obtain

$$\lim_{n\to\infty} \left| \frac{\Delta_{n+1}}{\Delta_n} \right| = \prod_{i=1}^{d} \max\{1, |x_i|\}.$$

This looks very much like the infinite part of the height![2] If A is an irreducible monic polynomial without roots on the unit circle we get

$$\lim_{n\to\infty} \left| \frac{\Delta_{n+1}}{\Delta_n} \right| = M(A) = e^{\deg(A)h(x)} = e^{[\mathbb{Q}(x):\mathbb{Q}]h(x)},$$

where x is any root of A. In order to avoid trivialities we also set $x \neq 0$.
Surely x is not a root of unity. Kronecker's Theorem 3.3.14 implies that $h(x) > 0$, i.e., $M(A) > 1$.
In any case $|\Delta_n|$ increases exponentially with rate $M(A) = e^{[\mathbb{Q}(x):\mathbb{Q}]h(x)} > 1$.
Considering $A = X^3 - X - 1$ with its root $x > 1$ and in view of Example 3.2.9 we get

$$\frac{\Delta_{58}}{\Delta_{57}} = \frac{12117361}{9137329} = 1.326138\ldots \quad \text{where} \quad M(A) = e^{3h(x)} = x = 1.324717\ldots.$$

The difference $0.0014\ldots$ is very small.
Lehmer posed the following problem in 1933:

Problem (Lehmer)**.** For an arbitrary $\epsilon > 0$ find a polynomial $A \in \mathbb{Z}[X]$ with

$$1 < M(A) < 1 + \epsilon,$$

or, equivalently, find an algebraic number x with

$$0 < [\mathbb{Q}(x) : \mathbb{Q}]h(x) < \epsilon.$$

This is still **open**. The smallest known positive value of $[\mathbb{Q}(x) : \mathbb{Q}]h(x)$ has already been found by Lehmer himself. It is given by any root x of

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1,$$

[2] The limit exists also if no x_i is a root of unity.

where $[\mathbb{Q}(x):\mathbb{Q}] = 10$ and

$$10h(x) = 0.1623576120077381394\ldots.$$

For $y^3 = y + 1$ as in Example 3.11 we have

$$3h(y) = 0.2811995743229618465\ldots$$

which is much worse.
He has also shown that for algebraic numbers the degree $10, 12$ and 14 no smaller value occurs.
Let x be an algebraic integer and $A = X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$ be its minimal polynomial.
We go back to the proof of Northcott's Theorem 3.3.11 and assume that $[\mathbb{Q}(x):\mathbb{Q}]h(x) < \log 2$. Setting $d = [\mathbb{Q}(x):\mathbb{Q}]$ and $B = h(x)$ we find $dB < \log 2$ and $|a_k| \leq e^{2\log(2)d} = 4^d$. The number of possibilities for the polynomial A is therefore $\leq (2 \cdot 4^d + 1)^d$. This (very large) bound grows superexponentially in d and suggests that for a large d it is very time-consuming to tackle Lehmer's problem.
With a computer one could prove that there is no better example than Lehmer's one with degree < 56.[3] It is quite astonishing that Lehmer has found it without any help from a computer.
Based on these and other indications, it is now believed that Lehmer's problem cannot be solved. Hence one has the following conjecture (which is often wrongly attributed to Lehmer).

Conjecture. *There exists $c > 0$, such that, for any algebraic number x, we have either $h(x) = 0$ or $h(x) \geq c/[\mathbb{Q}(x):\mathbb{Q}]$.*

Not the following simple fact.

Lemma 3.4.2. *Let x be an algebraic number that is not an integer. Then we have $[\mathbb{Q}(x):\mathbb{Q}]h(x) \geq \log 2$.*

Proof. The leading coefficient of the polynomial from Definition 3.1.2 is at least 2. The claim then follows. □

Therefore, only algebraic integers are relevant for Lehmer's problem.
The best known general lower bound is due to Dobrowolski.

Theorem 3.4.3 (Dobrowolski)**.** *There exists $c > 0$, such that, for any algebraic number x, we have either $h(x) = 0$ or*

$$h(x) \geq \frac{c}{d}\left(\frac{\log\log d}{\log d}\right)^3,$$

where $d = [\mathbb{Q}(x):\mathbb{Q}]$.

[3] until 2008.

3.5 The Northcott and the Bogomolov properties

We now describe some recent results about heights of algebraic numbers.

Definition 3.5.1. Let $S \subseteq \overline{\mathbb{Q}}$.

1. We say that S has the **Northcott property** or simply property (N) if, for every $B > 0$, the set $\{\alpha \in S : h(\alpha) \leq B\}$ is finite.
2. We say that S has the **Bogomolov property** or simply property (B) if, there exists a real number C such that if $\alpha \in S$ has $h(\alpha) < C$, then $h(\alpha) = 0$.

Remark 3.5.2. It is clear that property (N) implies property (B).

Example 3.5.3. Here are some simple examples and facts.

1. It is an easy consequence of Nothcott's Theorem that any number field has both properties (N) and (B).
2. The elements of the sequence $\{2^{1/d}\}$ have decreasing positive height and therefore $\overline{\mathbb{Q}}$ does not have properties (N) nor (B).
3. The field $\mathbb{Q}^{\mathrm{ab}}$ that is the compositum of all cyclotomic extensions[4] does not have property (N) for obvious reasons.

Theorem 3.5.4 (Bombieri, Zannier)**.** *The compositum of all quadratic extensions of $\mathbb{Q}$, i.e, the field $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{3}, \dots)$, has property (N) (and therefore also (B)).*

Definition 3.5.5. An algebraic number α is called **totally real** if all embeddings $\mathbb{Q}(\alpha) \to \mathbb{C}$ are real. The union of all totally real algebraic numbers is a subfield of $\overline{\mathbb{Q}}$ that we indicate by $\mathbb{Q}^{\mathrm{tr}}$.

Theorem 3.5.6 (Schinzel)**.** *The field $\mathbb{Q}^{\mathrm{tr}}$ has property (B). In particular, for $\alpha \in \mathbb{Q}^{\mathrm{tr}} \setminus \{0, \pm 1\}$ we have*

$$h(\alpha) \geq h\left(\frac{1+\sqrt{5}}{2}\right) = \frac{1}{2}\log\left(\frac{1+\sqrt{5}}{2}\right)$$

Theorem 3.5.7 (Amoroso, Dvornicich)**.** *The field $\mathbb{Q}^{\mathrm{ab}}$ has property (B).*

Theorem 3.5.8 (Habegger)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. The field $\mathbb{Q}(E^{\mathrm{tors}})$, obtained by adjoining to $\mathbb{Q}$ the coordinates of all points of finite order of E, has property (B).*

3.6 Multiplicative dependent points on a line

We now use the Weil height to investigate certain Diophantine equations.

Definition 3.6.1. Let K be a field and let $x_1, \dots, x_n \in K^\times$. We say that they are **multiplicatively dependent** if there exists a vector $(a_1, \dots, a_n) \in \mathbb{Z}^n \setminus \{0\}$ such that

$$x_1^{a_1} \dots x_n^{a_n} = 1.$$

If such a vector does not exist we say that they are **multiplicatively independent**.

[4] By the Kronecker-Weber theorem this is the maximal abelian extension of $\mathbb{Q}$.

Example 3.6.2. We are going to consider multiplicatively dependent solutions x, y of the equation $x + y = 1$.
The pair $x = 1/2$ and $y = 1/2$ is clearly multiplicatively dependent, since $xy^{-1} = 1$.
Moreover, $x = -1$ and $y = 2$ are also multiplicatively dependent because $x^2y^0 = 1$.
Together with $(2, -1)$, these give at least three rational pairs (x, y) with x, y multiplicatively dependent and $x + y = 1$.
If we consider algebraic solutions, we clearly have infinitely many. Indeed, if $x \neq 1$ is a root of unity and $y = 1 - x$, we have $x^r y^0 = 1$, where r is the order of x.

Theorem 3.6.3. *Let $x, y \in \overline{\mathbb{Q}}^\times$ be multiplicatively dependent algebraic numbers with $x + y = 1$. Then we have $h(x), h(y) \leq \log 4$.*

Proof. The proof is based on an idea by E. Bombieri.
By symmetry we may assume that $h(x) \geq h(y)$. We must then show that $h(x) \leq \log 4$.
Without loss of generality we may also assume that $h(x) > 0$.
There are $(r, s) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$ with $x^r y^s = 1$, and thus $x^r = y^{-s}$. By Lemma 3.3.3 we have

$$|r|h(x) = |s|h(y).$$

If $s = 0$, then $r \neq 0$ and this implies $h(x) = 0$, which we excluded. Therefore, $s \neq 0$ and thus we can consider $q = r/s \in \mathbb{Q}$, which satisfies

$$|q| = \frac{h(y)}{h(x)} \leq 1.$$

By Lemma 3.3.6 it follows that $h(x) = h(1 - y) \leq h(1) + h(-y) + \log 2 = h(y) + \log 2$, since $h(y) = h(-y)$. By symmetry we have $h(y) \leq h(x) + \log 2$ and therefore

$$|h(x) - h(y)| \leq \log 2.$$

Substituting $h(y)$ by $|q|h(x)$ we find $h(x)\,|1 - |q|| \leq \log 2$.
There are then two cases.
If $|q| \leq 1/2$, then $|1 - |q|| = 1 - |q| \geq 1/2$ and therefore $h(x) \leq 2 \log 2 = \log 4$ and we are done.
The second case is $|q| > 1/2$. Here we make a multiplicative coordinate trasformation. We define

$$\tilde{x} = x^{-1} \quad \text{and} \quad \tilde{y} = x^{-1}y.$$

We know that $h(\tilde{x}) = h(x^{-1}) = h(x)$ and therefore it is sufficient to show that $h(\tilde{x}) \leq \log 4$.
Since $x^r y^s = 1$, we must have that $\tilde{x}$ and $\tilde{y}$ are also multiplicatively dependent. More specifically,

$$\tilde{x}^{-r-s}\tilde{y}^s = x^{r+s}(x^{-1}y)^s = x^r y^s = 1.$$

This is a non-trivial relation since $s \neq 0$. We proceed as above and obtain $|-r-s|h(\tilde{x}) = |s|h(\tilde{y})$ or simply $|\tilde{q}|h(\tilde{x}) = h(\tilde{y})$ where $\tilde{q} = -r/s - 1 = -q - 1$.

Moreover, we have $\tilde{x} - \tilde{y} = x^{-1}(1-y) = 1$ and we find again as above

$$h(\tilde{x})\,|1 - |\tilde{q}|| = |h(\tilde{x}) - h(\tilde{y})| \leq \log 2. \tag{3.16}$$

As $|q| \leq 1$, we have $q + 1 \geq 0$, and thus $|\tilde{q}| = q + 1$ and $|1 - |\tilde{q}|| = |q|$. But we were in the case $|q| > 1/2$ and therefore it follows from (3.16) that we have $h(\tilde{x}) \leq 2 \log 2$. □

Corollary 3.6.4. *Let $x, y \in \mathbb{Q}^\times$ be multiplicatively dependent rational numbers with $x + y = 1$. Then*

$$(x, y) \in \{(1/2, 1/2), (-1, 2), (2, -1)\}.$$

Proof. Write $x = a/b$ with $a, b \in \mathbb{Z}$ coprime and $b \neq 0$. By Theorem 3.6.3 we have that $|a| \leq 4$ and $|b| \leq 4$. Therefore, we can just try case by case all possible x and $y = 1 - x$. For every candidate one establishes whether x and y are multiplicatively dependent by looking at the prime factorization. For instance, $x = 3/4$ has height $\log 4$. Thus $y = 1 - x = 1/4$, but $3/4$ and $1/4$ are not multiplicatively dependent since

$$\left(\frac{3}{4}\right)^r \left(\frac{1}{4}\right)^s = 3^r 4^{-r-s}$$

is equal to 1 only in case $r = s = 0$.
In this way one finds that there are only the three solutions listed above. □

Exercise 3.6.5. What happens if we replace $x + y$ by another linear form?

The above theorem is a special case of a general result by Bombieri, Masser and Zannier.

Theorem 3.6.6 (Bombieri, Masser, Zannier [2])**.** *Let $f_1, \ldots, f_n \in \overline{\mathbb{Q}}(X)$ be non-zero rational functions such that there is no non-zero vector $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ with*

$$f_1^{a_1} \cdots f_n^{a_n} = c$$

for some $c \in \overline{\mathbb{Q}}^\times$. Then the set

$$\{\alpha \in \overline{\mathbb{Q}} : f_1(\alpha), \ldots, f_n(\alpha) \text{ are multiplicatively dependent}\}$$

is a set of bounded height. Moreover, there exist at most finitely many $\alpha \in \overline{\mathbb{Q}}$ such that there are two linearly independent $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{Z}^n$ such that

$$f_1^{a_1}(\alpha) \cdots f_n^{a_n}(\alpha) = f_1^{b_1}(\alpha) \cdots f_n^{b_n}(\alpha) = 1.$$

Using a result of Frey that was a generalization of Theorem 3.5.8 it is possible to prove the following result.

Theorem 3.6.7 (Barroero, Sha)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. There is an effectively computable constant $C = C(E)$ such that, if (x, y) is a torsion point of E such that x and y are multiplicatively dependent, then (x, y) has order at most C.*

The important point of the above statement is the word "effective". In mathematics, prominently in number theory, the adjective effective attached to a certain quantity means that, in principle, this quantity can be computed. In the above theorem this means that one could sit down, be given an E and, after a finite (though probably astronomical) number of computations, "spit out" the real number $C(E)$ satisfying the property described in the statement. This would also allow to list all points (x, y) with x and y multiplicatively dependent.

4 Runge's Theorem

4.1 The statement

In this chapter we are going to use the Weil height to prove a version of Runge's Theorem.

Theorem 4.1.1 (Runge)**.** *Let $F \in \mathbb{Q}[X,Y] \setminus \mathbb{Q}$ be a polynomial that is irreducible in $\overline{\mathbb{Q}}[X,Y]$ and is of the form*

$$F = F_h + B$$

where F_h is homogeneous of degree $\deg F_h = \deg F > \deg B$. We assume moreover that $\deg_X F_h = \deg_Y F_h = \deg F$ and that F_h possesses two irreducible factors $P, Q \in \mathbb{Q}[X,Y]$ with $P/Q \notin \mathbb{Q}$. Then,

$$\{(x,y) \in \mathbb{Z} \times \mathbb{Q} : F(x,y) = 0\}$$

is finite.

Example 4.1.2.

(i) Consider

$$F = Y^2 - X^2 + X - 1.$$

Note that F satisfies the hypotheses of the above theorem. There are integral solutions, e.g., $(0,-1),(0,1),(1,-1),(1,1)$. The decomposition from Runge's theorem is

$$F_h = Y^2 - X^2 = (Y-X)(Y+X) \quad \text{and} \quad B = X - 1.$$

and $P = Y - X$ and $Q = Y + X$ are the factors of F_h.

(ii) On the other hand, many interesting examples are not covered by Runge's Theorem. It is consequence of a theorem of Siegel that, for a fixed $k \in \mathbb{Z} \setminus \{0\}$, the equation

$$y^2 = x^3 + k$$

has at most finitely many solutions $(x,y) \in \mathbb{Z}^2$. Consider $F = Y^2 - X^3 - k$. We have $F_h = -X^3$ so F violates the condition $\deg_X F_h = \deg_Y F_h$ and the hypothesis on the existence of irreducible factors that are not proportional.

4.2 The resultant

Before we turn to the proof of Runge's Theorem, we need some prior knowledge about the resultants of two polynomials.

The resultant answers the following (algebraic) question. Let K be a field and F and G two polynomials in $K[X,Y]$. What can be said about the set of their common zeros

$$\{(x,y) \in K^2 : F(x,y) = G(x,y) = 0\}?$$

We can partially answer the question with the help of the resultant.

Definition 4.2.1. Let R be a ring (commutative with 1) and $d \geq 1, e \geq 1$ be integers. Let $F = f_0X^d + f_1X^{d-1} + \cdots + f_d$ and $G = g_0X^e + g_1X^{e-1} + \cdots + g_e$ be two polynomials in $R[X]$. The (d,e)**-resultant** or simply **resultant** of F and G is

$$\mathrm{Res}_{d,e}(F,G) = \det \begin{pmatrix} f_0 & f_1 & f_2 & \cdots & f_d & & & \\ & f_0 & f_1 & \cdots & f_{d-1} & f_d & & \\ & & \ddots & & & & \ddots & \\ & & & f_0 & f_1 & \cdots & & f_d \\ g_0 & g_1 & g_2 & \cdots & g_e & & & \\ & g_0 & g_1 & \cdots & g_{e-1} & g_e & & \\ & & \ddots & & & & \ddots & \\ & & & g_0 & g_1 & \cdots & & g_e \end{pmatrix} \in R. \tag{4.1}$$

The first e rows of the matrix contain the coefficients of f and the last d rows contain the coefficients of g. It is a $d+e \times d+e$ Matrix. If $d = 0$ and $e \geq 1$ we set $\mathrm{Res}_{d,e}(F,G) = f_0^e$ while if $d \geq 1$ and $e = 0$ we set $\mathrm{Res}_{d,e}(F,G) = g_0^d$.

For the interested reader we suggest [3].

Example 4.2.2. (i) Let $F = aX^2 + bX + c$ and $G = F' = 2aX + b$. We have

$$\mathrm{Res}_{2,1}(F,G) = \det \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix} = -a(b^2 - 4ac).$$

Up to the factor $-a$ the resultant of F and G is the discriminant of F.

(ii) The definition of the resultant does not require that d be the degree of F or that e be the degree of G. Let F and G be as in (i). Then $\mathrm{Res}_{d,e}(F,G)$ is well defined as long as $d \geq 2$ and $e \geq 1$. For instance, for $d = 3, e = 1$, we have

$$\mathrm{Res}_{3,1}(F,G) = \det \begin{pmatrix} 0 & a & b & c \\ 2a & b & 0 & 0 \\ 0 & 2a & b & 0 \\ 0 & 0 & 2a & b \end{pmatrix} = 2a^2(b^2 - 4ac). \tag{4.2}$$

but $\mathrm{Res}_{3,2}(F,G) = 0$, since the first column of the matrix we must consider is zero. Therefore, the resultants depend on (d,e). The natural choice, however, is $d = \deg F$ and $e = \deg G$ if both polynomials are not constant.

Exercise 4.2.3. Calculate the following $\mathrm{Res}_{d,e}(F,G)$:

1. $F = X^2 + X + 1$, $G = X^2 - 2$, $d = e = 2$ and $R = \mathbb{Z}$.
2. $F = X^2 + Y^2 - 1$, $G = XY - 1$, $d = 2$, $e = 1$ and $R = \mathbb{Q}[Y]$.

Lemma 4.2.4. *Let R be an integral domain and $F, G \in R[X] \setminus \{0\}$ be polynomials with $d = \deg F$ and $e = \deg G$ and $(d, e) \neq (0, 0)$. There exist $A, B \in R[X]$ with $\deg A < \deg G, \deg B < \deg F$ and $(A, B) \neq (0, 0)$ such that*

$$AF + BG = \mathrm{Res}_{d,e}(F, G).$$

Proof. We assume that R is an integral domain to be able to use linear algebra in the quotient field of R.
Suppose $d = 0$ and $e \geq 1$. Then $\mathrm{Res}_{d,e}(F, G) = F^e = F^{e-1}F + 0G$ and we have our claim. The case $e = 0$ and $d \geq 1$ is analogous.
We now assume $d, e \geq 1$. After multiplying by powers of X, we get exactly $e + d$ non homogeneous linear equations

$$\begin{aligned}
X^{e-1}F &= f_0X^{d+e-1} + f_1X^{d+e-2} + \cdots + f_d \quad X^{e-1} \\
X^{e-2}F &= \qquad f_0X^{d+e-2} + \cdots + f_{d-1}X^{e-1} + \quad f_dX^{e-2} \\
&\vdots \qquad\qquad \ddots \qquad\qquad \ddots \\
F &= \qquad\qquad\qquad\qquad\qquad\qquad f_0X^d + \cdots + f_d \\
X^{d-1}G &= g_0X^{d+e-1} + g_1X^{d+e-2} + \cdots + g_e \quad X^{d-1} \\
X^{d-2}G &= \qquad g_0X^{d+e-2} + \cdots + g_{e-1}X^{d-1} + \quad g_eX^{d-2} \\
&\vdots \qquad\qquad \ddots \qquad\qquad \ddots \\
G &= \qquad\qquad\qquad\qquad\qquad\qquad g_0X^e + \cdots + g_e.
\end{aligned}$$

We can write these equalities in matrix form in the following way: we have $y = \mathcal{M}x$, where $\mathcal{M}$ is the $(d + e) \times (d + e)$ matrix in (4.1), x is the column vector with entries $(X^{d+e-1}, X^{d+e-2}, \ldots, 1)$ and y is the column vector

$$(X^{e-1}F, X^{e-2}F, \ldots, F, X^{d-1}G, X^{d-2}G, \ldots, G).$$

In particular, $\det \mathcal{M} = \mathrm{Res}_{d,e}(F, G)$.
If $r_1, \ldots, r_{d+e}$ are the columns of $\mathcal{M}$, then we can write $y = \mathcal{M}x$ as

$$y = r_1X^{d+e-1} + r_2X^{d+e-2} + \cdots + r_{d+e}.$$

We now use the fact that the determinant is linear in the columns and that matrices with two proportional columns are singular, to get

$$\det \mathcal{M} = \det(r_1, r_2, \ldots, r_{d+e-1}, y).$$

We now calculate the determinant $\det(r_1, r_2, \ldots, r_{d+e-1}, y)$ with respect to the last column and obtain

$$\begin{aligned}
\mathrm{Res}_{d,e}(F, G) = \det \mathcal{M} &= \delta_0X^{e-1}F + \cdots + \delta_{e-1}F + \delta_eX^{d-1}G + \cdots + \delta_{d+e-1}G \\
&= \underbrace{(\delta_0X^{e-1} + \cdots + \delta_{e-1})}_{=A}F + \underbrace{(\delta_eX^{d-1} + \cdots + \delta_{d+e-1})}_{=B}G
\end{aligned}$$

where $\delta_0, \dots, \delta_{d+e-1} \in R$ are minors of $\mathcal{M}$.
Now, to prove that $(A, B) \neq (0, 0)$ we use the fact that R is an integral domain. We may certainly assume that $\operatorname{Res}_{d,e}(F, G) = 0$ otherwise $A \neq 0$ or $B \neq 0$ must hold. In this case the determinant of $\mathcal{M}$ vanishes. Since R is an integral domain we may use linear algebra in its quotient field. There exists a row vector $\delta = (\delta_0, \dots, \delta_{d+e-1}) \in R^{d+e} \setminus \{0\}$ with $\delta\mathcal{M} = 0$. By $y = (X^{e-1}F, X^{e-2}F, \dots, F, X^{d-1}G, X^{d-2}G, \dots, G) = \mathcal{M}x$, after multiplying on the left by δ, we find the equality

$$\underbrace{(\delta_0 X^{e-1} + \cdots + \delta_{e-1})}_{=A} F + \underbrace{(\delta_e X^{d-1} + \cdots + \delta_{d+e-1})}_{=B} G = 0,$$

which was what we had to show. □

We partially answer the above question.

Lemma 4.2.5. *Let K be a field and $F, G \in K[X, Y] \setminus K$ polynomials with F irreducible and $F \nmid G$. Let L be a field extension of K. Then, the set of common roots $\{(x, y) \in L^2 : F(x, y) = G(x, y) = 0\}$ is finite.*

Proof. It suffices to prove the lemma under the assumption that G is irreducible.
Let $d = \deg_X F$ and $e = \deg_X G$.
We may assume $(d, e) \neq (0, 0)$, otherwise F and G have a common root if and only if they have a common divisor which contradicts our hypothesis.
We apply Lemma 4.2.4 on the integral domain $R = K[Y]$. There are then $A, B \in K[Y][X] = K[Y, X]$, not both zero, such that $\deg_X B < \deg_X F$ and $AF + BG = \operatorname{Res}_{d,e}(F, G) = P \in K[Y]$
We want to exclude that $AF + BG = P = 0$. Suppose this holds. We have $A \neq 0$ or $B \neq 0$ by Lemma 4.2.4. If $B = 0$, then $AF = 0$, but this would contradict $A \neq 0$ as $F \neq 0$. Similarly, $B \neq 0$. Therefore $F \mid BG$. Since $K[X, Y]$ is a unique factorization domain, the irreducible polynomial F must be a divisor of B or G. Since $\deg_X B < \deg_X F$ and $B \neq 0$ it follows that $F \mid G$, a contradiction.
We then have $AF + BG = P \in K[Y] \setminus \{0\}$ is a polynomial in only the variable Y.
If $(x, y) \in L^2$ is a common root of F and G, then

$$P(y) = A(x, y)F(x, y) + B(x, y)G(x, y) = 0.$$

But P has at most finitely many roots y and therefore we have finitely many possibilities for y. A symmetrical argument tells us that the same holds for the set of possible x and the lemma is proved. □

Corollary 4.2.6. *Let R be a unique factorization domain and $F, G \in R[X] \setminus R$ be polynomials of degree d and e. If $\operatorname{Res}_{d,e}(F, G) = 0$, then F and G have a common divisor in $R[X]$ of positive degree.*

Proof. By Lemma 4.2.4 there are $A, B \in R[X]$ with $AF + BG = 0$ where $\deg A \leq e - 1$ and $\deg B \leq d - 1$ and $(A, B) \neq 0$. It is clear that $A \neq 0$ and $B \neq 0$ and thus $F \mid BG$. We know that $R[X]$ is factorial so $F = F_1F_2$ for some polynomials $F_1, F_2 \in R[X]$ with $F_1 \mid B$ and $F_2 \mid G$. By $\deg F > \deg B$ we must have $\deg F_2 \geq 1$. Therefore, F_2 is the divisor we were looking for. □

4.3 A height inequality

Runge proved his result using power series of algebraic functions.
Our proof of Runge's Theorem relies on a height inequality.

Remark 4.3.1. As always, $\overline{\mathbb{Q}}$ denotes an algebraic closure of $\mathbb{Q}$.

(i) Let $m \geq 1$ and $n \geq 1$ be integer and and $F = X^m - Y^n$. Let $x, y \in \overline{\mathbb{Q}}$ be algebraic numbers such that $F(x, y) = 0$. Therefore $x^m = y^n$. By Lemma 3.3.1(i) we have

$$mh(x) = nh(y). \tag{4.3}$$

(ii) Consider another relation $F(x, y) = 0$, where $F = Y^2 - X^3 - 1$, meaning $y^2 = x^3 + 1$. Do we have $3h(x) = 2h(y)$? In general not. Indeed one can take for instance $x = 2$ and $y = 3$, but $3 \log 2 \neq 2 \log 3$.
On the other hand, by Lemma 3.3.1(i) and Lemma 3.3.6 we have $2h(y) = h(y^2) = h(x^3 + 1) \leq h(x^3) + h(1) + \log 2 = 3h(x) + \log 2$. Conversely wa have $3h(x) = h(x^3) = h(y^2 - 1) \leq 2h(y) + \log 2$ after analogous computations. It follows

$$|3h(x) - 2h(y)| \leq \log 2.$$

(iii) Let $F \in \overline{\mathbb{Q}}[X, Y] \setminus \overline{\mathbb{Q}}$ be irreducible with $m = \deg_X F$ and $n = \deg_Y F$. Let $x, y \in \overline{\mathbb{Q}}$ with $F(x, y) = 0$. We have seen in (ii) that in general $mh(x)$ and $nh(y)$ are different.
An important step in the proof of Runge's theorem is realizing that $h(x)$ and $h(y)$ are not independent. Roughly speaking we are going to see that

$$mh(x) \approx nh(y),$$

for some appropriate definition of $\approx$.

We prove the following theorem for irreducible polynomials.

Theorem 4.3.2. *Let K be a number field and $F \in K[X, Y] \setminus K$ be an irreducible polynomial with $m = \deg_X(F)$ and $n = \deg_Y(F)$. For all $\epsilon > 0$ there exists a constant $C(F, \epsilon) \geq 0$ such that*

$$|mh(x) - nh(y)| \leq \epsilon(h(x) + h(y)) + C(F, \epsilon)$$

for all $x, y \in \overline{\mathbb{Q}}$ with $F(x, y) = 0$.

Example 4.3.3. Why do we have the hypothesis that F is irreducible? Without any further assumption on F the difference $mh(x) - nh(y)$ may not be bounded, as the following example shows. Let $F = (X^2 - Y)(Y^2 - X)$ and note $\deg_X F = 3 = \deg_Y F$. Then $F(x, x^2) = 0$ for all $x \in \overline{\mathbb{Q}}$, but

$$\deg_X(F)h(x) - \deg_Y(F)h(x^2) = 3(h(x) - 2h(x)) = -3h(x)$$

is not bounded independently of $h(x)$, as $h(x)$ is arbitrarily large.

Remark 4.3.4.
In case $m = 0$, then F is a polynomial in the variable Y. In this case $F(x, y) = 0$ means that y lies in a finite set that depends only on F while x is arbitrary. We then trivially have

$$|0h(x) - nh(y)| = nh(y) \leq C(F)$$

for $C(F)$ sufficiently large. So our theorem is correct for $m = 0$. In a completely analogous way, one shows that it is true for $n = 0$.

First we construct an auxiliary polynomial with the help of linear algebra.

Lemma 4.3.5. *Let K be a field and $F \in K[X, Y]$ a polynomial with $m = \deg_X(F)$ and $n = \deg_Y(F) \geq 1$. Let $d, l \in \mathbb{N}$ be parameters with $d > m, l > n$ and $ml < nd$. There are polynomials $R, S \in K[X, Y]$ with*

$$\max\{\deg_X(R), \deg_X(S)\} < d, \quad \max\{\deg_Y(R), \deg_Y(S)\} < n \tag{4.4}$$

such that $RY^l - S = FB$ for some polynomial $B \in K[X, Y] \setminus \{0\}$.

Proof. We consider the set

$$\big\{B \in K[X, Y] : \deg_X(B) < d - m \text{ and } \deg_Y(B) < l\big\}.$$

This is a K-vector space of dimension $(d - m)l$. For all polynomials B in this vector space, FB is a polynomial with $\deg_X(FB) = \deg_X(F) + \deg_X(B) < m + (d - m) = d$ and $\deg_Y(FB) = \deg_Y(F) + \deg_Y(B) < n + l$. Now, the law $B \mapsto FB$ defines an injective linear map with image

$$\begin{aligned} V &= \big\{FB : B \in K[X, Y], \deg_X(B) < d - m \text{ und } \deg_Y(B) < l\big\} \\ &\subseteq W = \big\{H \in K[X, Y] : \deg_X(H) < d \text{ and } \deg_Y(H) < n + l\big\} \end{aligned}$$

and $\dim V = (d - m)l$.
It is enough to show that V contains a non-zero element of the form $RY^l - S$ with R, S as in (4.4). For an element in W to be of this form, the coefficient of X^iY^j must be 0 for all $0 \leq i < d$ and $n \leq j < l$. These are exactly $d(l - n)$ linear conditions.
Therefore, the set

$$U = \{H \in W : H \text{ of the form } RY^l - S \text{ with (4.4)}\}$$

is a vector subspace of W with $\dim U = \dim W - d(l - n)$.
By linear algebra we have

$$\dim V + \dim U = \dim(V + U) + \dim(V \cap U) \leq \dim W + \dim(V \cap U).$$

We obtain

$$\dim(V \cap U) \geq \dim V + \dim U - \dim W = \dim V - d(l - n) = (d - m)l - d(l - n) = dn - ml$$

which is positive by hypothesis.
Therefore $V \cap U$ is not trivial and there is $RY^l - S$ of the form FB with R and S as wanted. □

Proof of Theorem 4.3.2. Now K is a number field and $F \in K[X,Y]$ is irreducible. By Remark 4.3.4 we may assume that $m = \deg_X F \geq 1$ and $n = \deg_Y F \geq 1$.
We introduce parameters $d, l \in \mathbb{N}$ that satisfy $d > m, l > n$ and

$$\frac{m}{n} < \frac{d}{l}.$$

There are then polynomials $R, S \in K[X,Y]$ as in Lemma 4.3.5. In particular, the polynomial $RY^l - S$ is a multiple of F. We have

$$\max\{\deg_X(R), \deg_X(S)\} < d \quad \text{and} \quad \max\{\deg_Y(R), \deg_Y(S)\} < n. \tag{4.5}$$

By Proposition 2.2.12 we may assume that R and S have coefficients in $\mathcal{O}_K$.
Let now $x, y \in \overline{\mathbb{Q}}$ with $F(x,y) = 0$. It follows that

$$R(x,y)y^l = S(x,y). \tag{4.6}$$

We choose a number field $L \supseteq K$ that contains x and y. For any place $v \in M(L)$ there are two possibilities.

Case 1. The place v is finite. As $R \in \mathcal{O}_K[X]$, its coefficients have v-adic absolute value at most 1. The ultrametric inequality and the degree inequality (4.5) imply that

$$|R(x,y)|_v \leq \max\{1, |x|_v\}^{d-1} \max\{1, |y|_v\}^{n-1}.$$

The same upper bound holds for $|S(x,y)|_v$.

Case 2. The place v is infinite and comes from an embedding $\sigma : L \to \mathbb{C}$. We write $C_{d,l}$ for the maximum of $|\tau(r_{ij})|, |\tau(s_{ij})|$, where r_{ij}, s_{ij} are the coefficients of R and S and $\tau : L \to \mathbb{C}$ varies among all field embeddings. The constant $C_{d,l}$ depends on F and on d, l, but we only mention d and l in the index. Now we can employ the usual triangle inequality and obtain

$$|R(x,y)|_v = |\sigma(R(x,y))| \leq ndC_{d,l} \max\{1, |x|_v\}^{d-1} \max\{1, |y|_v\}^{n-1},$$

as R has at most nd non-zero coefficients. Analogously wa have the same bound for $|S(x,y)|_v$.

We can put everything together in the following inequality

$$\max\{|R(x,y)|_v, |S(x,y)|_v\} \leq \max\{1, |x|_v\}^{d-1} \max\{1, |y|_v\}^{n-1} \begin{cases} 1 & : v \in M^0(K), \\ ndC_{d,l} & : v \in M^\infty(K). \end{cases}$$

We now assume that $R(x,y) \neq 0$. By the product formula (Proposition 2.5.18) applied to $R(x,y)$ we have

$$\begin{aligned} \sum_{v \in M(L)} d_v \log \max\left\{1, \frac{|S(x,y)|_v}{|R(x,y)|_v}\right\} &= \sum_{v \in M(L)} d_v \log \max\{|R(x,y)|_v, |S(x,y)|_v\} \\ &\leq \left(\sum_{v \in M(L)} d_v \log\left(\max\{1, |x|_v\}^{d-1} \max\{1, |y|_v\}^{n-1}\right) \right) + \underbrace{\sum_{v \in M^\infty(L)} d_v \log(ndC_{d,l})}_{=[L:\mathbb{Q}] \log(ndC_{d,l})}. \end{aligned}$$

We divide this expression by $[L:\mathbb{Q}]$. On the left hand side we have $h(S(x,y)/R(x,y))$ while on the right we find $(d-1)h(x)+(n-1)h(y)+\log(ndC_{d,l})$. Using (4.6) we have

$$lh(y) = h\left(\frac{S(x,y)}{R(x,y)}\right) \leq (d-1)h(x)+(n-1)h(y)+\log(ndC_{d,l}).$$

We bring $h(y)$ to the left and divide by $l-n+1>0$ and get

$$h(y) \leq \frac{d-1}{l-n+1}h(x)+\frac{1}{l-n+1}\log(ndC_{d,l}).$$

We may choose d and l as we want as long as they satisfy the conditions above. Recall that m and n are fixed and we also have a fixed positive real number ϵ.
We can find d and l with

$$\frac{m}{n} < \frac{d}{l} \leq \frac{m}{n}\left(1+\frac{\epsilon}{2}\right).$$

Moreover, for $l>n$ sufficiently large, we have that

$$1-\frac{n}{l} \geq \frac{1+\frac{\epsilon}{2}}{1+\epsilon}.$$

We fix a choice of d and l satisfying these conditions. We have

$$\frac{d-1}{l-n+1} < \frac{d}{l-n} = \frac{d}{l}\frac{1}{(1-n/l)} \leq \frac{m}{n}\left(1+\frac{\epsilon}{2}\right)\frac{1+\epsilon}{1+\frac{\epsilon}{2}} = \frac{m}{n}(1+\epsilon)$$

It follows that

$$h(y) \leq \frac{m}{n}(1+\epsilon)h(x)+C', \tag{4.7}$$

where C' is a constant depending on the choice of d and l and on F. As we have chosen d and l depending on ϵ, the constant C' depends actually on ϵ and F.
We have proved this inequality under the assumption $R(x,y)\neq 0$. What happens when this value vanishes? Then we have $F(x,y)=R(x,y)=0$ and we can use Lemma 4.2.5. By hypothesis F is irreducible in $K[X,Y]$ and R cannot be constant. Moreover, recall that $\deg_Y R < n = \deg_Y F$, so R cannot be a multiple of F. It follows that F and R may have at most finitely many common roots $(x,y)\in\overline{\mathbb{Q}}^2$. We then possibly enlarge C' so that (4.7) holds also in this case.
It follows that, after replacing ϵ by ϵ/m,

$$nh(y) \leq mh(x)+\epsilon h(x)+nC' \leq mh(x)+\epsilon(h(x)+h(y))+nC'.$$

The analogous inequality with x in place of y follows by symmetry and we have proved our theorem. □

Corollary 4.3.6. *Let K, F be as in Theorem 4.3.2 with $m=\deg_X(F)$ and $n=\deg_Y(F)$. Suppose $n\geq 1$. For all $\epsilon>0$ there exists a constant $C(F,\epsilon)\geq 0$ such that*

$$h(y) \leq \left(\frac{m}{n}+\epsilon\right)h(x)+C(F,\epsilon)$$

for all $x,y\in\overline{\mathbb{Q}}$ with $F(x,y)=0$.

Proof. We have proved this in (4.7) above. □

4.4 Proof of Runge's Theorem

Let us recall the statement of Runge's Theorem.

Theorem 4.4.1 (Runge)**.** *Let $F \in \mathbb{Q}[X,Y] \setminus \mathbb{Q}$ be a polynomial that is irreducible in $\overline{\mathbb{Q}}[X,Y]$ and is of the form*

$$F = F_h + B$$

where F_h is homogeneous of degree $\deg F_h = \deg F > \deg B$. We assume moreover that $\deg_X F_h = \deg_Y F_h = \deg F$ and that F_h possesses two irreducible factors $P, Q \in \mathbb{Q}[X,Y]$ with $P/Q \notin \mathbb{Q}$. Then F has at most finitely many integral roots, meaning

$$\{(x,y) \in \mathbb{Z} \times \mathbb{Q} : F(x,y) = 0\}$$

is finite.

Proof. The dehomogenized polynomials $P(X,1)$ and $Q(X,1)$ belong to $\mathbb{Q}[X]$ and their roots are contained in some number field $K \subseteq \overline{\mathbb{Q}}$. Over $K[X,Y]$ we have the factorizations

$$P(X,Y) = p_0 \prod_{i=1}^{a} (X - \alpha_i Y) \quad \text{and} \quad Q(X,Y) = q_0 \prod_{i=1}^{b} (X - \beta_i Y).$$

We have

$$\{\alpha_1, \dots, \alpha_a\} \cap \{\beta_1, \dots, \beta_b\} = \emptyset,$$

because P and Q are irreducible and $P/Q \notin \mathbb{Q}$. Moreover the α_i, β_i cannot be zero otherwise this would contradict $\deg_X F_h = \deg_Y F_h = \deg F$.
We introduce a new variable

$$Z = X - \alpha_1 Y \in K[X,Y],$$

and consider

$$\widehat{F} = F(X, (X - Z)/\alpha_1) \in K[X,Z].$$

This is irreducible since F is irreducible in $K[X,Y] \subset \overline{\mathbb{Q}}[X,Y]$ (the change of coordinates is invertible and does not change the irreducibility). The degree of $\widehat{F}$ with respect to X and Z is at most $d = \deg F$.
The homogeneous part of highest degree of $\widehat{F}$ has degree at most $d-1$ in X and therefore is divisible by Z and $\deg_Z \widehat{F} = d$.
Let $F(x,y) = 0$ with $x \in \mathbb{Z}, y \in \mathbb{Q}$. We set $z_1 = x - \alpha_1 y \in K$ and therefore $\widehat{F}(x, z_1) = 0$. By Corollary 4.3.6 we have

$$h(z_1) \leq \left(\frac{d-1}{d} + \epsilon \right) h(x) + C.$$

We choose $\epsilon = 1/(2d)$.
We may assume $x \neq 0$ since $F(0,Y)$ has degree d and has therefore at most d roots. Then, $h(x) = \log |x|$ and we get $h(z_1) \leq (1 - 1/(2d)) \log |x| + C$.

We now choose an embedding $\sigma : K \to \mathbb{C}$ such that $|\sigma(z_1)|$ is minimal. By definition we have

$$\log \max\{1, |\sigma(z_1)|\} \leq \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M^\infty(K)} d_v \log \max\{1, |z_1|_v\} \leq h(z_1),$$

and therefore

$$|x - \sigma(\alpha_1)y| = |\sigma(z_1)| \leq e^C |x|^{1-1/(2d)}. \tag{4.8}$$

The same argument for $z_2 = x - \beta_1 y$ gives

$$|x - \tau(\beta_1)y| = |\tau(z_2)| \leq e^C |x|^{1-1/(2d)}. \tag{4.9}$$

for some field embedding $\tau : K \to \mathbb{C}$.
Recall that $\alpha_1, \beta_1 \neq 0$ and that $P(X,1)$ and $Q(X,1)$ have no common roots. Then $\sigma(\alpha_1) \neq \tau(\beta_1)$ and both are non-zero. We may then eliminate y and obtain

$$x = \frac{\tau(\beta_1)\sigma(z_1) - \sigma(\alpha_1)\tau(z_2)}{\tau(\beta_1) - \sigma(\alpha_1)}.$$

By (4.8) and (4.9) it follows that $|x| \leq C'|x|^{1-1/(2d)}$ for some constant C' that is independent of x. Since $x \in \mathbb{Z}$ there are at most finitely many possibilities for x. For a fixed x, $F(x,Y)$ is not identically zero otherwise F would be a multiple of $X - x$ and this would contradict the hypotheses. Therefore there are at most finitely many possibilities for $y \in \mathbb{Q}$ associated to any x. □

4.5 A theorem by Skolem

Definition 4.5.1. Let K be a number field and $x, y \in K$ with $(x,y) \neq (0,0)$. We define

$$\operatorname{lgcd}(x,y) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M(K)} d_v \log \left(\frac{\max\{1, |x|_v, |y|_v\}}{\max\{|x|_v, |y|_v\}} \right).$$

Exercise 4.5.2. Prove that the above definition is independent of the choice of K.

Exercise 4.5.3. Let $x, y \in \mathbb{Z}$, not both zero. Show that $\operatorname{lgcd}(x,y) = \log \gcd(x,y)$.

Exercise 4.5.4. In Exercise 3.2.11 we have defined the height on projective spaces. Similarly we can define the height of a point $(x_1, \ldots, x_n) \in \overline{\mathbb{Q}}^n$:

$$h(x_1, \ldots, x_n) = h([1 : x_1 : \cdots : x_n]) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M(K)} d_v \log \max\{1, |x_1|_v, \ldots, |x_n|_v\}.$$

Prove that for $x, y \in \overline{\mathbb{Q}}$ and $x \neq 0$ we have

$$\operatorname{lgcd}(x,y) = h(x,y) - h(y/x).$$

In 1929 Skolem showed that if $P \in \mathbb{Z}[X,Y]$ is irreducible in $\mathbb{Q}[X,Y]$ and $P(0,0) = 0$, then there are only finitely many coprime $x, y \in \mathbb{Z}$ with $P(x,y) = 0$.
The aim of this section is to prove the following theorem, which has an immediate consequence for pairs of coprime integers that are solutions of a diophantine equation.

Theorem 4.5.5 (Skolem)**.** *Let K be a number field and $F \in K[X,Y]$ be an irreducible polynomial with $n = \deg_Y F \geq 1$. We assume that $F(0,0) = 0$ and $(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y})(0,0) \neq (0,0)$. Then, for all $\epsilon > 0$, there exists a constant $C = C(F,\epsilon)$ such that*

$$|n \cdot \operatorname{lgcd}(x,y) - h(x)| \leq \epsilon h(x) + C$$

for all $x, y \in \overline{\mathbb{Q}}$ with $F(x,y) = 0$ and $(x,y) \neq (0,0)$.

Example 4.5.6. Consider the equation

$$X^{2020} - Y^{2019} + X^{1728} - XY + X - Y = 0.$$

This satisfies the hypothesis of the above theorem. This, together with Exercise 4.5.3, implies that this equations has at most finitely many solutions $(x,y) \in \mathbb{Z}^2$ with x, y coprime.

First we compare $h(y/x)$ with $h(x)$ for $x \neq 0$.

Lemma 4.5.7. *Let K be a number field and $F \in K[X,Y]$ be an irreducible polynomial with $F(0,0) = 0$, $(\partial F/\partial X, \partial F/\partial Y)(0,0) \neq 0$, $n = \deg_Y F \geq 1$ and $d = \deg F$, the total degree of F. Then, for all $\epsilon > 0$ there exists a $C = C(F,\epsilon) \geq 0$ with*

$$|nh(y/x) - (d-1)h(x)| \leq \epsilon(h(x) + h(y)) + C$$

for all $x, y \in \overline{\mathbb{Q}}$ with $F(x,y) = 0$ and $x \neq 0$.

Proof. We write $F = \sum_{i,j} f_{ij} X^i Y^j$. The hypothesis $F(0,0) = 0$ means that $f_{00} = 0$ and moreover $(\partial F/\partial X(0,0), \partial F/\partial Y(0,0)) = (f_{10}, f_{01}) \neq (0,0)$.
We define

$$\widehat{F} = X^{-1} F(X, XZ) = \sum_{i,j} f_{ij} X^{i+j-1} Z^j.$$

Since $f_{00} = 0$, only terms with $i + j \geq 1$ appear, thus $\widehat{F}$ is a polynomial in $K[X,Z]$.
The degree $\deg_X \widehat{F}$ is exactly $d-1$, since there is a pair (i,j) with $f_{ij} \neq 0$ and $i + j = d$.
Moreover, $\deg_Z \widehat{F} = n$.
Let $(x,y) \in \overline{\mathbb{Q}}$ be a solution $F(x,y) = 0$ with $x \neq 0$. Then, $\widehat{F}(x,z) = 0$ where $z = y/x$.
We want to apply Theorem 4.3.2 but we need to show that $\widehat{F}$ is irreducible. Once we have done that we get

$$|(d-1)h(x) - nh(y/x)| \leq \frac{\epsilon}{2}(h(x) + h(y/x)) + C,$$

where C depends on F and ϵ. But on the right hand side we have $h(x) + h(y/x) \leq h(x) + h(y) + h(x) \leq 2(h(x) + h(y))$ and this proves the lemma.

We are then left to show that $\widehat{F}$ is irreducible. Suppose there are non-constant $G, H \in K[X, Z]$ with $\widehat{F} = GH$. Then

$$F(X,Y) = X\widehat{F}\left(X, \frac{Y}{X}\right) = XG\left(X, \frac{Y}{X}\right) H\left(X, \frac{Y}{X}\right). \tag{4.10}$$

Now, given a rational function $R(X,Y) \in K(X,Y)$, this can be written as

$$X^e \frac{P(X,Y)}{Q(X,Y)}$$

for some integer e and polynomials $P(X,Y), Q(X,Y) \in K[X,Y]$ with $X \nmid P(X,Y)$, $Q(X,Y)$. We define $\operatorname{ord}_X R(X,Y) = e$. It is easy to see that $\operatorname{ord}_X(R_1R_2) = \operatorname{ord}_X(R_1) + \operatorname{ord}_X(R_2)$ for any $R_1(X,Y), R_2(X,Y) \in K(X,Y)$.
Now, the irreducibility of F and (4.10) imply that $\operatorname{ord}_X(\widehat{F}(X, Y/X)) = -1$. We set $g = \operatorname{ord}_X G(X, Y/X)$ and $h = \operatorname{ord}_X H(X, Y/X)$. Then $g + h = -1$. We immediately note that we cannot have $(g,h) = (0,-1)$ or $(-1,0)$ otherwise (4.10) would contradict the irreducibility of $F(X,Y)$. We might then assume that $g \geq 1$ which implies that $X \mid G(X,Z) \mid \widehat{F}(X,Z)$. This is not possible because $(f_{10}, f_{01}) \neq (0,0)$ and f_{10} is the constant term of $\widehat{F}(X,Z)$ and f_{01} is the coefficient of Z. □

Next we compare $h(x,y)$ with $h(x)$.

Lemma 4.5.8. *Let K be a number field and $F \in K[X,Y]$ irreducible with $d = \deg F$. Suppose $n = \deg_Y F \geq 1$. For all $\epsilon > 0$ there exists a constant $C = C(F, \epsilon) \geq 0$ with*

$$|nh(x,y) - dh(x)| \leq \epsilon(h(x) + h(y)) + C$$

for all $x, y \in \overline{\mathbb{Q}}$ with $F(x,y) = 0$.

Proof. We first suppose that $\deg_X F = \deg F = d$.
Our polynomial F has the shape $\sum_{i,j} f_{ij} X^i Y^j$ with $f_{d0} \neq 0$, since $d = \deg F = \deg_X F$. Without loss of generality we may assume that F has coefficients in $\mathcal{O}_K$.
We now consider a number field L with $x, y \in L$ and $F(x,y) = 0$.
Let $v \in M(L)$. If v is a finite place we claim that $|x|_v \leq \max\{1, |f_{d0}|_v^{-1}\} \max\{1, |y|_v\}$. Suppose on the contrary that $|x|_v > \max\{1, |f_{d0}|_v^{-1}\} \max\{1, |y|_v\}$. Let $(i,j) \neq (d,0)$ with $f_{ij} \neq 0$. If $j = 0$ then $i \leq d-1$ and therefore

$$|f_{d0}x^d|_v \geq |f_{d0}x|_v |x^i|_v > |x|_v^i \geq |f_{i0}x^i|_v.$$

We have used here the fact that $f_{i,j} \in \mathcal{O}_K$ and thus $|x|_v > |f_{d0}|_v^{-1}$.
For $j \geq 1$, since $i + j \leq d$, we have

$$|f_{d0}x^d|_v \geq |f_{d0}|_v |x|_v^i |x|_v^j \geq |f_{d0}|_v^j |x|_v^i |x|_v^j > |x|_v^i |y|_v^j \geq |f_{ij}x^i y^j|_v.$$

We then have

$$|f_{d0}x^d|_v > |f_{ij}x^i y^j|_v$$

for all $(i,j) \neq (d,0)$. But $f_{d0}x^d = \sum_{(i,j)\neq(d,0)} -f_{ij}x^iy^j$ and the ultrametric inequality implies $|f_{d0}x^d|_v \leq \max_{(i,j)\neq(d,0)}\{|f_{ij}x^iy^j|_v\}$. This is a contradiction.
Let now v be an infinite place. Then, $|f_{d0}x^d|_v \leq C_1 \max_{(i,j)\neq(d,0)}\{|f_{ij}x^iy^j|_v\}$ for some constant C_1 depending only on d. This implies that

$$|x^d|_v \leq C_2 \max\{1, |f_{d0}|_v^{-1}\} \max_{(i,j)\neq(d,0)}\{|x^iy^j|_v\},$$

for some $C_2 \geq 1$ that depends on d and $|f_{ij}|_v$. If $|x|_v \geq \max\{1, |y|_v\}$, then $|x^iy^j/x^{d-1}|_v \leq |y|_v$ and we have

$$|x|_v \leq C_2 \max\{1, |f_{d0}|_v^{-1}\} \max\{1, |y|_v\},$$

but the same inequality clearly holds if $|x|_v \leq \max\{1, |y|_v\}$.
Putting everything together we have

$$|x|_v \leq \max\{1, |f_{d0}|_v\}^{-1} \max\{1, |y|_v\} \begin{cases} 1 & : \text{if } v \in M^0(L), \\ C_2 & : \text{if } v \in M^\infty(L). \end{cases}$$

We may replace the left hand side by $\max\{1, |x|_v, |y|_v\}$.
We take logarithms, multiply by d_v and sum over all $v \in M(L)$. We get

$$0 \leq h(x,y) - h(y) \leq C_3,$$

for some constant $C_3 \geq 0$ that only depends on F.
By Theorem 4.3.2 we have $|dh(x) - nh(x,y)| \leq \epsilon(h(x) + h(y)) + C_4$, where $C_4 \geq 0$ only depends on F and ϵ. This is our claim under the assumption $d = \deg_X F = \deg F$.
In general we have $\deg_X F \leq \deg F$. If the inequality is strict we perform a change of coordinates and set $z = \lambda x + y$ and

$$\widehat{F}(X,Z) = F(X, Z - \lambda X)$$

with $\lambda \in \mathbb{N}$. For λ sufficiently large in terms of F we have $\deg_X \widehat{F} = \deg F$ (see exercise below). Moreover we have $\deg_Z \widehat{F} = \deg_Y F = n$. The polynomial $\widehat{F}$ stays irreducible and we have $|dh(x) - nh(x, \lambda x + y)| \leq \epsilon(h(x) + h(y)) + C_5$. Finally, an easy application of the triangular inequality (see exercise below) shows that $|h(x,y) - h(x, \lambda x + y)| \leq C_6$, with C_6 independent of x, y. □

Exercise 4.5.9. Prove the claim we used above: there exists a $\lambda \in \mathbb{N}$ such that $\deg_X \widehat{F} = \deg F$.

Exercise 4.5.10. Fix $\lambda \in \mathbb{N}$. Prove that there exists a constant C_6 such that $|h(x,y) - h(x, \lambda x + y)| \leq C_6$ for all $x, y \in \overline{\mathbb{Q}}$.

Proof of Theorem 4.5.5. Let $x, y \in \overline{\mathbb{Q}}$. For $x = 0$ there is nothing to show, as $F(0,Y)$ is not identically zero and therefore there are at most finitely many roots for y.
We now assume $x \neq 0$. We have seen in Exercise 4.5.4 that $\operatorname{lgcd}(x,y) = h(x,y) - h(y/x)$. We have

$$\begin{aligned} |n \cdot \operatorname{lgcd}(x,y) - h(x)| &= |nh(x,y) - nh(y/x) - dh(x) + (d-1)h(x)| \\ &\leq |nh(x,y) - dh(x)| + |nh(y/x) - (d-1)h(x)|. \end{aligned}$$

We use Lemmas 4.5.8 and 4.5.7 and get a bound of the shape $\epsilon(h(x)+h(y))+C_1$.
We now use again Lemma 4.5.8 and get

$$|nh(x,y)-dh(x)| \leq \epsilon(h(x)+h(y))+C_2 \leq \epsilon(h(x)+h(x,y))+C_2$$

that implies, for a sufficiently small ϵ,

$$h(x,y) \leq C_3(h(x)+1),$$

for some constant C_3 depending only on F.
Finally

$$|n \cdot \operatorname{lgcd}(x,y)-h(x)| \leq \epsilon(h(x)+h(y))+C_1 \leq \epsilon(h(x)+h(x,y))+C_1 \leq \epsilon(h(x))+C_4,$$

and we have proved the theorem. □

4.6 An application toward Hilbert's Irreducibility Theorem

Let $F \in \mathbb{Q}[X,Y]$ be an irreducible polynomial with $\deg_Y P > 0$. A famous theorem of Hilbert states that $P(x,Y) \in \mathbb{Q}[Y]$ is irreducible for infinitely many integers x.
We prove the following variant of Hilbert's Irreducibility Theorem.

Theorem 4.6.1. *Let $F \in \mathbb{Q}[X,Y]$ be an irreducible polynomial with $\deg_Y F \geq 1$, $F(0,0)=0$ and $(\partial F/\partial X, \partial F/\partial Y)(0,0) \neq (0,0)$. For all sufficiently large prime number p, the polynomial $F(p,Y)$ is irreducible in $\mathbb{Q}[Y]$.*

Proof. We use Theorem 4.5.5.
As F has positive degree in Y, the degree of $F(x,Y)$ is $n = \deg_Y F$ for all but at most finitely many $x \in \overline{\mathbb{Q}}$. For a sufficiently large prime number p we then have $n = \deg_Y F(p,Y) \geq 1$. Let $y \in \overline{\mathbb{Q}}$ with $F(p,y)=0$. We must show that $[K:\mathbb{Q}]=n$ where $K=\mathbb{Q}(y)$. Without loss of generality we may assume $n \geq 2$.
We choose $\epsilon = 1/(2n)$ and apply Theorem 4.5.5 to get

$$|n \cdot \operatorname{lgcd}(p,y) - \log p| \leq \frac{\log p}{2n} + C. \tag{4.11}$$

This implies that, for p large enough we must have $\operatorname{lgcd}(p,y) > 0$. By Definition 4.5.1 it follows that there exists a place $v \in M(K)$ with

$$\max\{1, |p|_v, |y|_v\} > \max\{|p|_v, |y|_v\}.$$

This implies that $\max\{1,|p|_v,|y|_v\}=1$ and $|p|_v<1, |y|_v<1$ and therefore v is a finite place that corresponds to a prime ideal $P \subseteq \mathcal{O}_K$ with $p \in P$.

We have $|y|_v = p^{-\nu_P(y)/e(P)}$ or $y = 0$. In any case $|y|_v \leq p^{-1/e(P)}$. Moreover, $|p|_v = p^{-1} \leq p^{-1/e(P)}$. We then have

$$\log \frac{\max\{1, |p|_v, |y|_v\}}{\max\{|p|_v, |y|_v\}} = \log \frac{1}{\max\{|p|_v, |y|_v\}} \geq \frac{\log p}{e(P)}.$$

Every summand in $\operatorname{lgcd}(p, y)$ is non negative and

$$d_v \log \frac{\max\{1, |p|_v, |y|_v\}}{\max\{|p|_v, |y|_v\}} \geq f(P) \log p \geq \log p.$$

Therefore, $[K : \mathbb{Q}]\operatorname{lgcd}(p, y) \geq \log p$.
Together with (4.11) and $n \geq 2$ we get

$$\left(\frac{n}{[K : \mathbb{Q}]} - 1\right) \log p \leq n \cdot \operatorname{lgcd}(p, y) - \log p \leq |n \cdot \operatorname{lgcd}(p, y) - \log p| \leq \frac{\log p}{2n} + C.$$

If $[K : \mathbb{Q}] \leq n - 1$, then $n/[K : \mathbb{Q}] - 1 \geq n/(n-1) - 1 = 1/(n-1)$. We obtain

$$\frac{\log p}{n-1} \leq \frac{\log p}{2n} + C,$$

and therefore $p \leq e^{C/(1/(n-1)-1/(2n))}$ is bounded.
We conclude that there are at most finitely many p such that $[K : \mathbb{Q}] < n$. □

5 Arithmetic Dynamics

5.1 Introduction

Arithmetic dynamics deals with number theoretic properties of dynamical systems.
For the interested reader we suggest [9].
In the general setting, a dynamical system is given by a self-map

$$f : S \to S$$

for some set S.
Sequences of the form

$$s, f(s), f(f(s)), f(f(f(s))), \dots \tag{5.1}$$

for some element $s \in S$, are object of study. We call any such sequence **orbit** of s with respect to f.

- For which $s \in S$ is the sequence (5.1) finite?
- In case the sequence is infinite, how is it distributed in S, with respect to a metric, a topology or a measure?

In the extreme case of a fixed point $f(s) = s$, the orbit consists of only one element, but these sequences can also be infinite.
In this section we will mainly deal with polynomial and rational self-maps. The basic set S is typically a subset of a number field or the field of algebraic numbers.

Example 5.1.1. Consider $S = \mathbb{C}$ and $f(x) = x^2$ as self-map.
Let $x \in \mathbb{C}$. The orbit $x, f(x), f(f(x)), f(f(f(x))), \dots$ is

$$x, x^2, (x^2)^2 = x^4, ((x^2)^2)^2 = x^8, \dots, x^{2^n}, \dots$$

In case $x = 0$ the sequence is constantly 0 and is surely finite.
If $0 < |x| < 1$, the absolute value of the n-th entry is $|x|^{2^n}$ and it converges 0. The sequence is infinite.
If $|x| > 1$, the sequance of absolute values converges to ∞ and the orbit is again infinite.
We are only left with complex numbers on the unit circle.

Lemma 5.1.2. *Let $x \in \mathbb{C}$. The sequence $(x^{2^n})_{n\geq 0}$ is finite if and only if $x = 0$ or x is a root of unity.*

Proof. We have already dealt with the case $x = 0$. For a root of unity x, the powers of x lie in the finite group that x generates.
Let now $(x^{2^n})_{n\geq 0}$ be finite. Then, there are integers $n > m \geq 0$ with $x^{2^n} = x^{2^m}$. It follows that $x^{2^m}(x^{2^n-2^m} - 1)$. Therefore $x = 0$ or x is a root of unity. □

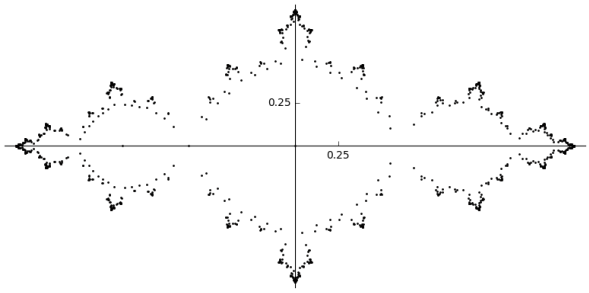


Figure 5.1: Roots of $f(f(f(f(f(f(f(f(f(f(x))))))))))) = x$ for $f = x^2 - 1$, degree $= 1024$

Example 5.1.3. We now consider $f = x^2 - 1$ and $S = \mathbb{Q}$.
The sequence starting with $s = 0$ is

$$0, -1, 0, -1, \ldots$$

and therefore finite. If we begin with $s = 1$ we find

$$1, 0, -1, 0, -1, \ldots.$$

But if we start with $s = 2$ we get

$$2, 3, 8, 63, 3968, \ldots.$$

It is not hard to see that the sequence is infinite.
The iterates of f are now difficult to write down

$$\begin{aligned} f(x) &= x^2 - 1, \\ f(f(x)) &= x^4 - 2x^2, \\ f(f(f(x))) &= x^8 - 4x^6 + 4x^4 - 1, \\ f(f(f(f(x)))) &= x^{16} - 8x^{14} + 24x^{12} - 32x^{10} + 14x^8 + 8x^6 - 8x^4, \\ &\vdots \end{aligned}$$

Figure 5.1 reflects such complicated behavior of the iterates.
We are going to see later that there are at most finitely many $s \in \mathbb{Q}$ such that

$$s, f(s), f(f(s)), f(f(f(s))), \ldots$$

is finite. The height plays an important role in this.

Definition 5.1.4. Let S be a set $f : S \to S$ a self-map.

(i) For an integer $n \geq 1$ we write $f^{\circ n} : S \to S$ for the self map defined by

$$f^{\circ n}(s) = (\underbrace{f \circ \cdots \circ f}_{n \text{ times}})(s)$$

for all $s \in S$. For $n = 0$ we set $f^{\circ n}(s) = s$.

(ii) Let $s \in S$. We call s a **periodic point** of f if there is an integer $n > 0$ with $f^{\circ n}(s) = s$. We call s a **preperiodic point** of f if there are integers $n > m \geq 0$ such that $f^{\circ n}(s) = f^{\circ m}(s)$. We indicate by $\mathrm{Per}(f, S)$ the subset of S of periodic points of S while $\mathrm{PrePer}(f, S)$ will indicate the set of preperiodic points of f.

Note that a point is preperiodic if and only if its orbit contains a periodic point.

Lemma 5.1.5. *Let S be a set, $f : S \to S$ a self-map and $s \in S$. Then s is a preperiodic point of f if and only if the set $\{f^{\circ n}(s) : n \geq 0\}$ is finite.*

Proof. The proof is similar to the one of Lemma 5.1.2 and left as an exercise. □

Exercise 5.1.6. We see some examples.

1. Let G be a group, $d \geq 2$ an integer and $f : G \to G$ be the d-th power map $f(g) = g^d$. Prove that $\mathrm{PrePer}(f, G) = G_{\mathrm{tors}}$ the set of elements of G of finite order.
2. Let S be a set and $f : S \to S$ a function.
   (a) If S is a finite set, prove that f is bijective if and only if $\mathrm{Per}(f, S) = S$.
   (b) In general, prove that if $\mathrm{Per}(f, S) = S$, then f is bijective.
   (c) Give an example of an infinite set S and map f with the property that f is bijective and $\mathrm{Per}(f, S) \neq S$.
   (d) If f is injective, prove that $\mathrm{PrePer}(f, S) = \mathrm{Per}(f, S)$.
3. Let $f(z) = z^d + a \in \mathbb{Z}[z]$ and let p be a prime number. Prove that $\mathrm{Per}(f, \mathbb{F}_p) = \mathbb{F}_p$ if and only if $\gcd(d, p - 1) = 1$.

Exercise 5.1.7. Let K be a number field with $K \subseteq \mathbb{C}$ and $f \in K[X]$ a polynomial of degree $\deg f \geq 2$. Let $x \in \mathbb{C}$ be a preperiodic point of f. Show that x is algebraic over K and that, if f is monic and has coefficients in $\mathcal{O}_K$, then it is an algebraic integer.

Exercise 5.1.8. Let $f \in \mathbb{C}[X]$ be a polynomial of degree $\deg f \geq 2$. Show that there exists an element of $\mathbb{C}$ that is not preperiodic for f.

5.2 Rational functions

Remark 5.2.1. In arithmetic dynamics we do not only use polynomial maps as $x \mapsto x^2$ or $x \mapsto x^2 - 1$ but also rational maps. The class of Lattès maps play an important role and we are going so say something about them later. An example is

$$f(x) = \frac{x^4 - 8x}{4x^3 + 4}.$$

Here one must be careful about the choice of the set S. We are not allowed to take $\overline{\mathbb{Q}}$ or $\mathbb{C}$, because the denominator vanishes at $-1, e^{\pm 2\pi i/6}$.

We must then see rational functions as self-maps of the projective line. In the following definitions we recall some notation.

Definition 5.2.2. Let K be a field and $n \geq 1$. Let $x = (x_0, \ldots, x_n), y = (y_0, \ldots, y_n) \in K^{n+1} \setminus \{0\}$. We write $x \sim y$ if there is a $\lambda \in K^\times$ with $x = \lambda y$. Clearly $\sim$ is an equivalence relation on $K^{n+1} \setminus \{0\}$. The K-rational points of the n-dimensional **projective space** are the equivalence classes of this relation:

$$\mathbb{P}^n(K) = (K^{n+1} \setminus \{0\})/\sim .$$

We write elements $p \in \mathbb{P}^n(K)$ as $p = [x_0 : \cdots : x_n]$ and call $(x_0, \ldots, x_n)$ **projective coordinates** of p; these are of course only defined up to scalar multiplication in $K^\times$.

Example 5.2.3. We are mostly interested in the case $n = 1$. For any field K we have

$$\mathbb{P}^1(K) = \{[1 : x] : x \in K\} \cup \{[0 : 1]\}.$$

The elements $[1 : x]$ $(x \in K)$ and $[0 : 1]$ are pairwise distinct. We can therefore identify K with a subset of $\mathbb{P}^1(K)$ by the map $x \mapsto [1 : x]$.

Definition 5.2.4. Let K be a number field and $p = [x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$. We have proved in Chapter 3 that the following

$$h(p) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M(K)} d_v \log \max\{|x_0|_v, \ldots, |x_n|_v\}$$

is independent of the choice of projective coordinates $(x_0, \ldots, x_n)$ of the point p and of the choice of number field. We then have a well defined **projective Weil Height** for points of $\mathbb{P}^n(\overline{\mathbb{Q}})$.

Note that, for $x \in \overline{\mathbb{Q}}$ we have $h(x) = h([1 : x])$.
In the following we associate to a rational function a self-map of the projective line.

Remark 5.2.5. Let K be a field and $P, Q \in K[X] \setminus \{0\}$ be coprime polynomials. We want to turn $P/Q \in K(X)$ into a self-map of $\mathbb{P}^1(K)$ so that we can iterate it.
We must take into account the roots of Q, meaning that we cannot take $S = K$.
We define $d = \max\{\deg P, \deg Q\}$ and $\overline{P}(U, V) = U^d P(V/U) \in K[U, V]$ as well as $\overline{Q}(U, V) = U^d Q(V/U) \in K[U, V]$.
We define our $f : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ by setting

$$f([x_0 : x_1]) = [\overline{Q}(x_0, x_1) : \overline{P}(x_0, x_1)].$$

We now show that this is a well-defined self-map of $\mathbb{P}^1(K)$ and, in some sense, extends the rational function P/Q We start with the second part.
For $[x_0 : x_1] \in \mathbb{P}^1(K)$ with $x_0 \neq 0$ we have

$$\overline{P}(x_0, x_1) = x_0^d P(x_1/x_0) \quad \text{and} \quad \overline{Q}(x_0, x_1) = x_0^d Q(x_1/x_0).$$

If $Q(x_1/x_0) \neq 0$ we have

$$\overline{P}(x_0, x_1)/\overline{Q}(x_0, x_1) = P(t)/Q(t)$$

where $t = x_1/x_0$.
We then have, for all $t \in K$ such that $Q(t) \neq 0$,

$$f([1:t]) = [1 : P(t)/Q(t)].$$

Let us now check that f is a well-defined self-map of $\mathbb{P}^1(K)$.
Let $(x_0, x_1) \in K^2 \setminus \{0\}$ be arbitrary. We claim that $\overline{P}(x_0, x_1)$ and $\overline{Q}(x_0, x_1)$ cannot both vanish.
If $x_0 \neq 0$ we set $t = x_1/x_0$. Suppose that $\overline{Q}(x_0, x_1) = \overline{P}(x_0, x_1) = 0$ so it follows that $P(t) = Q(t) = 0$. By hypothesis P, Q are coprime as elements of $K[X]$. We then get a contradiction and (x_0, x_1) is not a common root of $\overline{P}$ and $\overline{Q}$. We now assume that $x_0 = 0$ and write $P = p_0X^a + \cdots$ and $Q = q_0X^b + \cdots$ with $p_0q_0 \neq 0$. Surely we must have $x_1 \neq 0$. We have $\overline{P}(x_0, x_1) = \overline{P}(0, x_1) = p_0x_0^{d-a}x_1^a$ and $\overline{Q}(0, x_1) = q_0x_0^{d-b}x_1^b$. Since $d = a$ or $d = b$ one of these values must be different from 0.
Therefore $[\overline{Q}(x_0, x_1) : \overline{P}(x_0, x_1)]$ is a well-defined element of $\mathbb{P}^1(K)$. This point in invariant under the transformation $(x_0, x_1) \mapsto \lambda(x_0, x_1)$ with $\lambda \in K^\times$ because

$$(\overline{Q}(\lambda x_0, \lambda x_1), \overline{P}(\lambda x_0, \lambda x_1)) = \lambda^d(\overline{Q}(x_0, x_1), \overline{P}(x_0, x_1)).$$

We have showed above that $(\overline{Q}(x_0, x_1), \overline{P}(x_0, x_1)) \neq (0, 0)$, and therefore this point represents an element of $\mathbb{P}^1(K)$. Also we have seen that$f([x_0 : x_1]) = f([y_0 : y_1])$, if $[x_0 : x_1] = [y_0 : y_1]$. Therefore, $f : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ is well-defined.
We have seen that we may identify K with the subset $\{[1 : x] : x \in K\}$ of $\mathbb{P}^1(K)$. If $Q(x) \neq 0$, by virtue of this identification we will simply write

$$f(x) = P(x)/Q(x) \in K.$$

So f is a continuation of the rational function P/Q to $\mathbb{P}^1(K)$. There are no "singularities".
We call an f of this form a **rational map** of $\mathbb{P}^1(K)$ of degree d.

In what follows we are going to fix the map $K \to \mathbb{P}^1(K)$, $x \mapsto [1 : x]$. If f is a rational map of $\mathbb{P}^1$, $x \in K$ and $f([1 : x]) \neq [0 : 1]$ we just consider $f([1 : x]) = f(x)$ as an element of K.

Example 5.2.6. (i) The map $f(x) = x^2$ from Example 5.1.1 is also defined over $\overline{\mathbb{Q}}$. We know by Lemma 5.1.2 that the preperiodic points of f are exactly the roots of unity and 0. Therefore all $x \in \overline{\mathbb{Q}}$ we have

$$x \text{ is a preperiodic point of } f \iff h(x) = 0.$$

Moreover we have the functional equation.

$$h(f(x)) = h(x^2) = 2h(x).$$

(ii) For $f = x^2 - 1$ these properties do not hold anymore.
The golden ratio $x = (1 + \sqrt{5})/2$ satisfies $f(x) = x^2 - 1 = x$ and is therefore a fixed point of f. But

$$h\left(\frac{1+\sqrt{5}}{2}\right) = \frac{1}{2}\log\frac{1+\sqrt{5}}{2} > 0.$$

Moreover, in general we have $h(f(x)) \neq 2h(x)$. Therefore our height is not "compatible" with this f as it was for x^2.
But it is not hard to show that

$$|h(f(x)) - 2h(x)| \leq \log 2.$$

We have an "approximate" functional equation.

The following lemma is very important. It relates the heights of a point and its image under a rational map.

Lemma 5.2.7. *Let $f : \mathbb{P}^1(\overline{\mathbb{Q}}) \to \mathbb{P}^1(\overline{\mathbb{Q}})$ be a rational map of degree $d \geq 1$. There exists $c = c(f) \geq 0$ such that*

$$|h(f(p)) - dh(p)| \leq c$$

for all $p \in \mathbb{P}^1(\overline{\mathbb{Q}})$.

Proof. We identify $\overline{\mathbb{Q}}$ with $\{[1 : x] : x \in \overline{\mathbb{Q}}\} \subseteq \mathbb{P}^1(\overline{\mathbb{Q}})$. This identification is compatible with our height $h([1 : x]) = h(x)$. Now, let $P, Q \in \overline{\mathbb{Q}}[X] \setminus \{0\}$ be coprime polynomials such that $f([1 : x]) = [Q(x) : P(x)]$ for all $x \in \overline{\mathbb{Q}}$. We have $\max\{\deg P, \deg Q\} = d \geq 1$. There are at most finitely many $x \in \overline{\mathbb{Q}}$ such that $Q(x) = 0$. We may therefore assume that $p = [1 : x]$ with $x \in \overline{\mathbb{Q}}$ and $Q(x) \neq 0$. We have $f(p) = [1 : P(x)/Q(x)]$.
We write $P = p_0X^a + \cdots + p_a$ with $p_0 \neq 0$ and $Q = q_0X^b + \cdots + q_b$ with $q_0 \neq 0$.
Let K be a number field that contains x and all coefficients of P and Q and fix a $v \in M(K)$. The triangular inequality implies

$$|P(x)|_v \leq \max\{1, |a+1|_v\} \max\{|p_0|_v, \ldots, |p_a|_v\} \max\{1, |x|_v\}^a.$$

Analogously we have

$$|Q(x)|_v \leq \max\{1, |b+1|_v\} \max\{|q_0|_v, \ldots, |q_a|_v\} \max\{1, |x|_v\}^b,$$

Recall that $a, b \leq d$. As usual we take logarithms, multiply by d_v, sum over all $v \in M(K)$, divide by $[K : \mathbb{Q}]$ and get

$$h([Q(x) : P(x)]) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M(K)} d_v \log \max\{|Q(x)|_v, |P(x)|_v\} \leq dh(x) + c$$

for some constant $c \geq 0$ that is independent of x. We then have

$$h(f(p)) \leq dh(p) + c, \tag{5.2}$$

which gives the "easy" inequality.
We have to prove the inequality in the opposite direction.
As P and Q are coprime, there exist $A, B \in K[X]$ with $AP + BQ = 1$, by Lemma 4.2.4 and Corollary 4.2.6 [1]. We substitute X with V/U and multiply by U^d. We have

$$U^d = A(V/U)\underbrace{U^d P(V/U)}_{=\overline{P}(U,V)} + B(V/U)\underbrace{U^d Q(V/U)}_{=\overline{Q}(U,V)}.$$

Note that, on the right-hand side, U may appear in the denominator. Therefore, we multiply by U^e where $e = \max\{\deg A, \deg B\}$. Now we have

$$U^{d+e} = \underbrace{(U^e A(V/U))}_{=:\overline{A}}\overline{P}(U,V) + \underbrace{(U^e B(V/U))}_{=:\overline{B}}\overline{Q}(U,V)$$

We now substitute $(1, x)$ for (U, V) and use the triangular inequality to get

$$1 \le c'_v \max\{1, |x|_v\}^e \max\{|\overline{P}(1,x)|_v, |\overline{Q}(1,x)|_v\} \tag{5.3}$$

for all $v \in M(K)$. Here we have $c'_v \ge 1$ and $c'_v = 1$ for all $v \in M(K)$ except at most finitely many.
As we have seen in Remark 5.2.5, $\overline{P}(T,1)$ and $\overline{Q}(T,1)$ do not have any common root in $\overline{\mathbb{Q}}$. As before we have polynomials $A', B' \in K[T]$ such that

$$A'\overline{P}(T,1) + B'\overline{Q}(T,1) = 1.$$

We now substitute $T = U/V$ and multiply by V^d. As $\overline{P}$ and $\overline{Q}$ are homogeneous of degree d, we have that

$$A'(U/V)\overline{P}(U,V) + B'(U/V)\overline{Q}(U,V) = V^d$$

and

$$\underbrace{(V^g A'(U/V))}_{\in\overline{\mathbb{Q}}[U,V] \text{ of degree } g}\overline{P}(U,V) + \underbrace{(V^g B'(U/V))}_{\in\overline{\mathbb{Q}}[U,V] \text{ of degree } g}\overline{Q}(U,V) = V^{d+g}$$

where $g = \max\{e, \deg A', \deg B'\}$. Again we substitute $(1, x)$ for (U, V) and obtain as before

$$|x|_v^{d+g} \le c''_v \max\{1, |x|_v\}^g \max\{|\overline{P}(1,x)|_v, |\overline{Q}(1,x)|_v\},$$

where c''_v satisfies the same property as c'_v.
We combine this with (5.3) and find

$$\max\{1, |x|_v\}^{d+g} \le c'''_v \max\{1, |x|_v\}^g \max\{|\overline{P}(1,x)|_v, |\overline{Q}(1,x)|_v\},$$

where $c'''_v = \max\{c'_v, c''_v\}$ satisfies the same property as c'_v. We cancel $\max\{1, |x|_v\}^g$, take logarithms, multiply by d_v, sum over all $v \in M(K)$ and divide by $[K : \mathbb{Q}]$ to get

$$dh(p) = dh(x) \le \underbrace{h([P(x) : Q(x)])}_{h(f(p))} + \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M(K)} d_v \log(c'''_v).$$

The rightmost sum is a constant independent of x.
The lemma now follows by this and (5.2). □

[1] or maybe more elementarily, by Bezout's Identity.

5.3 The canonical height

We are going to construct a new height $\hat{h}_f : \overline{\mathbb{Q}} \to \mathbb{R}$ associated to any rational map f of $\mathbb{P}^1$ with $\deg f \geq 2$. This will vanish exactly at the preperiodic points of f and will satisfy the functional equation

$$\hat{h}_f(f(x)) = (\deg f)\hat{h}_f(x).$$

The following construction is due to Tate.

Lemma 5.3.1. *Let S be a set, $f : S \to S$ a self-map and $\varphi : S \to \mathbb{R}$ a function such that there are real numbers $d > 1$ and $c \geq 0$ with*

$$|\varphi(f(s)) - d\varphi(s))| \leq c,$$

for all $s \in S$. Then there exists a function $\hat{\varphi} : S \to \mathbb{R}$ such that

(i) We have

$$\lim_{n\to\infty} \frac{\varphi(f^{\circ n}(s))}{d^n} = \hat{\varphi}(s)$$

for all $s \in S$. In particular the limit exists.

(ii) We have

$$|\hat{\varphi}(s) - \varphi(s)| \leq \frac{c}{d-1} \quad \text{and} \quad \hat{\varphi}(f(s)) = d\hat{\varphi}(s)$$

for all $s \in S$.

(iii) For any $s \in S$ we have

$$s \text{ is a preperiodic point of } f \quad \Longrightarrow \quad \hat{\varphi}(s) = 0.$$

Proof. Let $s \in S$. We show that $(\varphi(f^{\circ n}(s))/d^n)_{n\geq 1}$ is a Cauchy sequence. The limit value defines the value $\hat{\varphi}(s)$ and this will prove (i).
Let $n > m \geq 0$ be integers. We construct a telescopic sum

$$\frac{\varphi(f^{\circ n}(s))}{d^n} - \frac{\varphi(f^{\circ m}(s))}{d^m} = \sum_{k=0}^{n-m-1} \left(\frac{\varphi(f^{\circ(m+k+1)}(s))}{d^{m+k+1}} - \frac{\varphi(f^{\circ(m+k)}(s))}{d^{m+k}} \right).$$

We use the triangular inequality and use the fact that $f^{\circ(m+k+1)} = f \circ f^{\circ(m+k)}$. It follows that

$$\left| \frac{\varphi(f^{\circ n}(s))}{d^n} - \frac{\varphi(f^{\circ m}(s))}{d^m} \right| \leq \sum_{k=0}^{n-m-1} \left| \frac{\varphi(f(f^{\circ(m+k)}(s)))}{d^{m+k+1}} - \frac{\varphi(f^{\circ(m+k)}(s))}{d^{m+k}} \right|.$$

By hypothesis we have $|\varphi(f(t)) - d\varphi(t)| \leq c$ for all $t \in S$. We substitute $t = f^{\circ(m+k)}(s)$ and find $|\varphi(f(f^{(m+k)}(s))) - d\varphi(f^{(m+k)}(s))| \leq c$. We divide this by d^{m+k+1} and obtain

$$\left| \frac{\varphi(f^{\circ n}(s))}{d^n} - \frac{\varphi(f^{\circ m}(s))}{d^m} \right| \leq \sum_{k=0}^{n-m-1} \frac{c}{d^{m+k+1}} \leq \frac{c}{d^{m+1}} \sum_{k=0}^{\infty} \frac{1}{d^k} = \frac{c}{d^{m+1}} \frac{1}{1-1/d}. \tag{5.4}$$

The right hand side can be made as small as wanted by choosing m sufficiently large. It follows that $(\varphi(f^{\circ n}(s))/d^n)_{n\geq 1}$ is a Cauchy sequence and we have (i).
To prove (ii) we take the limit as $n \to \infty$ in (5.4). By the definition of $\hat{\varphi}$ we have

$$\left|\hat{\varphi}(s) - \frac{\varphi(f^{\circ m}(s))}{d^m}\right| \leq \frac{c}{d^m(d-1)}$$

for all $m \geq 0$. The inequality in (ii) follows by choosing $m = 0$, since $f^{\circ 0}(s) = s$ by definition.
We now evaluate $\hat{\varphi}$ in $f(s)$ and find

$$\hat{\varphi}(f(s)) = \lim_{n\to\infty} \frac{\varphi(f^{\circ n}(f(x)))}{d^n} = \lim_{n\to\infty} d\frac{\varphi(f^{\circ(n+1)}(x))}{d^{n+1}} = d\hat{\varphi}(f(s)).$$

This gives the second part of (ii).
We now get to (iii). We use the identity

$$\hat{\varphi}(f^{\circ n}(s)) = d^n\hat{\varphi}(s),$$

which holds for all $s \in S$ and all integers $n \geq 0$ and can be proved by induction on n using (ii).
If s is preperiodic there are integers $n > m \geq 0$ with $f^{\circ n}(s) = f^{\circ m}(s)$. We apply $\hat{\varphi}$ and get $d^n\hat{\varphi}(s) = d^m\hat{\varphi}(s)$ Since $d > 1$ and $n > m$ we must have $\hat{\varphi}(s) = 0$ and we are done. □

Exercise 5.3.2. Let S, f, φ, d and c be as above. Let $\tilde{\varphi}\colon S \to \mathbb{R}$ be a function that satisfies the following properties:
(i) For all $s \in S$ we have $\tilde{\varphi}(f(s)) = d\tilde{\varphi}(s)$.
(ii) There exists $C \geq 0$, such that $|\tilde{\varphi}(s) - \varphi(s)| \leq C$ for all $s \in S$.
Prove that $\tilde{\varphi} = \hat{\varphi}$

Example 5.3.3. In case $f = x^2 - 1$ we know that

$$|h(f(x)) - dh(x)| \leq c = \log 2$$

for all $x \in \overline{\mathbb{Q}}$, where $d = 2$. We get a new height

$$\hat{h}_f = \hat{h}_{x^2-1} : \overline{\mathbb{Q}} \to \mathbb{R}$$

with the following properties.
We have

$$\hat{h}_f(x^2 - 1) = 2\hat{h}_f(x) \tag{5.5}$$

for all $x \in \overline{\mathbb{Q}}$ and

$$|\hat{h}_f(x) - h(x)| \leq \log 2.$$

Moreover, this new height must vanish at the preperiodic points of f.

Definition 5.3.4. Let $f : \mathbb{P}^1(\overline{\mathbb{Q}}) \to \mathbb{P}^1(\overline{\mathbb{Q}})$ be a rational map of degree $d \geq 2$. By Lemma 5.2.7 and Lemma 5.3.1(i) with $S = \mathbb{P}^1(\overline{\mathbb{Q}})$ and $\varphi = h$ the limit

$$\hat{h}_f(p) = \lim_{n\to\infty} \frac{h(f^{\circ n}(p))}{d^n}$$

exists for all $p \in \mathbb{P}^1(\overline{\mathbb{Q}})$. We call $\hat{h}_f : \mathbb{P}^1(\overline{\mathbb{Q}}) \to \mathbb{R}$ the **Call-Silverman height** or **canonical height** with respect to f. For $x \in \overline{\mathbb{Q}}$ we also write $\hat{h}_f(x) = \hat{h}_f([1 : x])$.

Example 5.3.5. (i) Let $P = X^2$ and $Q = 1$, and f be the rational map associated to P/Q. We know that $h(x^{2^n}) = 2^n h(x)$. Therefore, the canonical height $\hat{h}_{x^2}$ coincides with the usual h.

(ii) For other polynomials or rational functions f it is usually hard to calculate the value of the canonical height.

Exercise 5.3.6. Let $f = x^2 - 1$. Show that $\hat{h}_f(1/a) = \log|a|$ for every integer $a \neq 0$.

Theorem 5.3.7. *Let K be a number field and f a rational map of $\mathbb{P}^1(K)$ of degree $d \geq 2$. Then $\mathrm{PrePer}(f, \mathbb{P}^1(K))$ is a finite set.*

Proof. By Lemma 5.3.1(iii) we know that $\hat{h}_f(p) = 0$ for all $p \in \mathrm{PrePer}(f, \mathbb{P}^1(K))$. Let $p = [w : x]$ be such a point with $w, x \in K$. By part (ii) of the same lemma it follows that $h([w : x]) = |\hat{h}_f(p) - h([w : x])| \leq c$, where c depends only on f. If $w \neq 0$ we may assume that $w = 1$ and then $h([1 : x]) = h(x) \leq c$ By Northcott's Theorem, Theorem 3.3.11, there are at most finitely many such x and therefore at most finitely many preperiodic $[w : x]$ with $w \neq 0$. Clearly we only have one point with $w = 0$ and this gives only at most one additional preperiodic point. Therefore, the set of preperiodic points of f in $\mathbb{P}^1(K)$ is finite. □

Example 5.3.8. (i) Let $f(x) = x^2 + a$ with $a \in \mathbb{Q}$. A simple computation with the help of Lemma 3.3.6 shows that

$$h(x^2 + a) \leq 2h(x) + h(a) + \log 2.$$

Moreover,

$$2h(x) = h(x^2 + a - a) \leq h(x^2 + a) + h(a) + \log 2.$$

Therefore,

$$|h(x^2 + a) - 2h(x)| \leq h(a) + \log 2.$$

A possible choice for the constant c in Lemma 5.3.1 is then $c = (h(a) + \log 2)$.
Let $x \in \mathbb{Q}$ be a preperiodic point of f. By Lemma 5.3.1 (ii) and (iii) it follows that $h(x) \leq c = h(a) + \log 2$.
This means that the bound for $h(x)$ depends on a and we can explicitly determine all preperiodic x for a given a.

(ii) We can then ask ourselves the following question. How many preperiodic points can the map $x \mapsto x^2 + a$ have in $S = \mathbb{Q}$? This number depends on a.
For $a = 0$ there are only $0, \pm 1$, and the number is 3 in this case.
For $a = -29/16$ one can find the following complete list[2] of eight preperiodic points

$$\pm\frac{1}{4}, \pm\frac{3}{4}, \pm\frac{5}{4} \pm \frac{7}{4}.$$

Actually, we do not know of any $a \in \mathbb{Q}$ for which x^2+a has more than 8 preperiodic points in $\mathbb{Q}$.

Conjecture (Poonen)**.** *Let $a \in \mathbb{Q}$, then $x \mapsto x^2 + a$ has at most eight preperiodic point in $\mathbb{Q}$.*

The amazing thing about the conjecture is that the bound does not depend on the parameter a. Poonen formulated a more general conjecture about quadratic polynomials of which the above conjecture is a consequence.

Exercise 5.3.9. Let $c \in \mathbb{C}$ and $t_0 = (1 + \sqrt{1 + 4|c|})/2$. Let $z \in \mathbb{C}$ be a preperiodic point of $x \mapsto x^2 + c$. Show that $|z| \leq t_0$.

For the Call-Silverman height we can prove the converse of Lemma 5.3.1(iii). The following theorem is a generalization of Kronecker's Theorem, Theorem 3.3.14.

Theorem 5.3.10. *Let f be a rational map of $\mathbb{P}^1(\overline{\mathbb{Q}})$ of degree $d \geq 2$. For $p \in \mathbb{P}^1(\overline{\mathbb{Q}})$ we have*

$$p \in \mathrm{PrePer}(f, \mathbb{P}^1(\overline{\mathbb{Q}})) \quad \Longleftrightarrow \quad \hat{h}_f(p) = 0.$$

Proof. The implication "$\Longrightarrow$" follows form Lemma 5.3.1(iii).
Let $\hat{h}_f(p) = 0$ for a $p = [x : y] \in \mathbb{P}^1(\overline{\mathbb{Q}})$. We choose a number field K such that $x, y \in K$ and f is a rational map of $\mathbb{P}^1(K)$ (see the beginning of the proof of Lemma 5.2.7). For every integer $n \geq 0$ we have

$$\hat{h}_f(f^{\circ n}(p)) = d^n \hat{h}_f(p) = 0.$$

Since f is a rational map of $\mathbb{P}^1(K)$ we have $f^{\circ n}(p) = p_n \in \mathbb{P}^1(K)$. Now, for the n such that $p_n \neq [0 : 1]$, we let $p_n = [1 : x_n]$ with $x_n \in K$. Then, for these n, by Lemma 5.3.1(ii), we have $h([1 : x_n]) = h(x_n) \leq c$ where c depends only on f. Thus, Northcott's Theorem, Theorem 3.3.11, implies that the orbit of p is finite and therefore thare are $n > m \geq 0$ with $f^{\circ n}(p) = f^{\circ m}(p)$. Therefore, p is preperiodic. □

5.4 Lattès maps

Example 5.4.1. Let K be a number field and $a, b \in K$ with $4a^3 + 27b^2 \neq 0$. The homogeneous polynomial

$$Y^2Z - (X^3 + aXZ^2 + bZ^3)$$

[2]We do not count the point $[0 : 1]$.

defines an elliptic curve E in the projective plane. We indicate by $E(K)$ the set

$$E(K) = \{[x : y : z] \in \mathbb{P}^2(K) : y^2z = x^3 + axz^2 + bz^3\}.$$

It is a non-trivial fact that $E(K)$ has the structure of an abelian group where the operation $+$ is defined by homogeneous polynomials and $[0 : 1 : 0]$ is the neutral element. We define a map $\pi : E(K) \to \mathbb{P}^1(K)$ via $\pi([x : y : z]) = [x : z]$ for $[x : y : z] \neq [0 : 1 : 0]$ and $\pi([0 : 1 : 0]) = [1 : 0]$.
Moreover, the rational function

$$\frac{X^4 - 2aX^2 - 8bX + a^2}{4X^3 + 4aX + 4b} \tag{5.6}$$

defines a self-map $f = f_{a,b} : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ as in Remark 5.2.5.
We call such f a **Lattès map**. The duplication map $p \mapsto p + p$ defines a self-map $E(K) \to E(K)$ and this fits in the following commutative diagram

$$\begin{array}{ccc} E(K) & \xrightarrow{\text{duplication}} & E(K) \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{P}^1(K) & \xrightarrow{f} & \mathbb{P}^1(K) \end{array}$$

The fact that $4a^3 + 27b^2 \neq 0$ guaranties that numerator and denominator in (5.6) are coprime polynomials. This can be verified using the resultant.
We then have the Call-Silverman height $\hat{h}_f : \mathbb{P}^1(K) \to \mathbb{R}$ with $d = 4$ as in Definition 5.3.4. We indicate the composition $\hat{h}_f \circ \pi$ with $\hat{h}_E$. This height is usually called Néron-Tate height.
For $p \in E(K)$, it is not hard to prove that

$$\hat{h}_E(p + p) = \hat{h}_E(2p) = 4\hat{h}_E(p)$$

and

$$\hat{h}_E(p) = 0 \quad \iff \quad p \text{ has finite order in the group } E(K).$$

Therefore, the points of finite order of $E(K)$ are related to the preperiodic points of $f_{a,b}$.

The study of points of finite order on an elliptic curve has a long history and served as a motivation for the development of arithmetic dynamics. So we can hope to find out a lot about preperiodic points from Lattès maps.

Theorem 5.4.2 (Mazur 1977, 1978)**.** *Let E be an elliptic curve with $a, b \in \mathbb{Q}$. Then we have*

$$\#\{P \in E(\mathbb{Q}) : P \text{ has finite order}\} \leq 16.$$

The amazing thing about Mazur's theorem is the fact that the bound 16 is independent of the coefficients a, b. This difficult theorem was generalized to number field some time later.

Theorem 5.4.3 (Merel 1996)**.** *Let K be a number field with $D = [K : \mathbb{Q}]$ and E an elliptic curve with $a, b \in K$. Then,*

$$\#\{P \in E(K) : P \text{ has finite order}\} \leq B(D)$$

where $B(D)$ depends only on D.

As a consequence of Merel's Theorem we have the following corollary for Lattès maps.

Corollary 5.4.4. *Let K be a number field and $D = [K : \mathbb{Q}]$. There exists a constant $B(D)$ with the following property. For $a, b \in K$ with $4a^3 + 27b^2 \neq 0$ and f as in (5.6), the number of preperiodic points in $\mathbb{P}^1(K)$ of $f_{a,b}$ is bounded by $B(D)$.*

We conclude with a Conjecture that strongly generalizes the corollary.

Conjecture (Morton-Silverman)**.** *Let K be a number field and $f : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map of degree $d \geq 2$. Then*

$$\#\{p \in \mathbb{P}^1(K) : p \text{ is preperiodic for } f\}$$

is bounded by a function of $[K : \mathbb{Q}]$ and d.

6 Diophantine Equations in roots of unity

6.1 Introduction

The goal of this chapter is to solve Diophantine Equations in roots of unity.
It is very easy to see that there are exactly two pairs of roots of unity (ζ, ξ) that satisfy

$$\zeta + \xi = 1.$$

Let now $\eta \in \mathbb{C}$ be a root of unity. Every polynomial of the form

$$P = X^r Y^s - \eta$$

with $(r, s) \in \mathbb{Z}^2 \setminus \{0\}$ and $r \geq 0, s \geq 0$ has infinitely many solutions in roots of unity and the same holds for $X^r - \eta Y^s$.
In the '60s Ihara, Serre and Tate proved the converse of this assertion. We recall that μ_∞ denotes the subgroup of $\mathbb{C}^\times$ whose elements are the roots of unity.
We are going to prove a generalization of the following result.

Theorem 6.1.1 (Ihara, Serre, Tate)**.** *Let $P \in \mathbb{Q}[X, Y]$ be a polynomial such that*

$$\{(\zeta, \xi) \in \mu_\infty^2 : P(\zeta, \xi) = 0\}$$

is infinite. There there are integers $r \geq 0$ and $s \geq 0$, not both zero, such that P is not coprime with a polynomial of the form $X^r Y^s - 1$ or $X^r - Y^s$.

Exercise 6.1.2. Show that $F = 2XY - X - Y + 2$ has infinitely many solutions in $S^1 \times S^1$ where $S^1 = \{z \in \mathbb{C} : |z| = 1\}$.

6.2 Some Galois theory of cyclotomic fields

In this section we recall and collect a couple of basic facts about Galois theory of cyclotomic fields
Let φ be Euler φ-function. Let $\zeta \in \mu_\infty$ of order n. Then we know that the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is normal with $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. In particular, this isomorphism is very explicit

$$\begin{aligned} (\mathbb{Z}/n\mathbb{Z})^\times &\to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\ a &\mapsto (\zeta \mapsto \zeta^a) \end{aligned}$$

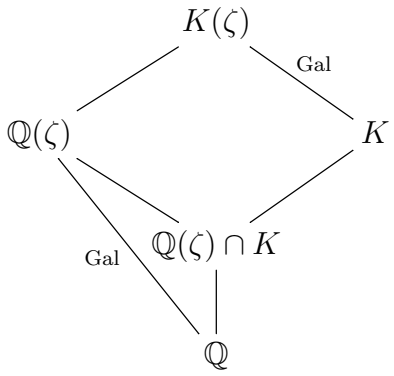
It is easy to see that, if K is a number field, then $K(\zeta)/K$ is normal. We use some basic Galois theory to prove the following fact.

Proposition 6.2.1. *Let $K \subseteq \mathbb{C}$ be a number field and $\zeta \in \mu_\infty$ of order n. Let $a \in \mathbb{Z}$ be coprime with n. Then, there exists $\sigma \in \mathrm{Gal}(K(\zeta)/K)$ such that $\sigma(\zeta) = \zeta^{a^t}$, where $t = [K \cap \mathbb{Q}(\zeta) : \mathbb{Q}] \leq [K : \mathbb{Q}]$.*

Proof. The group homomorphism

$$\begin{aligned} \iota : \mathrm{Gal}(K(\zeta)/K) &\to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \\ \sigma &\mapsto \sigma|_{\mathbb{Q}(\zeta)}. \end{aligned}$$

is clearly injective and therefore allows us to see $H = \mathrm{Gal}(K(\zeta)/K)$ as a subgroup of $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. We now consider the following diagram



Now, the image of ι is contained in $\{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) : \sigma|_{\mathbb{Q}(\zeta)\cap K} = \mathrm{id}_{\mathbb{Q}(\zeta)\cap K}\} = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta) \cap K)$. Moreover, if $\mathbb{Q}(\zeta)^H = \{\alpha \in \mathbb{Q}(\zeta) : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$ (which is equal to $\mathbb{Q}(\zeta)\cap K$) then, by Corollary 3.5 of [5] we have $H = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)^H) = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta) \cap K)$.
Therefore, we have that $[K(\zeta) : K] = [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta)\cap K]$ and the index of H in G satisfies

$$[G : H] = \frac{[\mathbb{Q}(\zeta) : \mathbb{Q}]}{[K(\zeta) : K]} = \frac{[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta) \cap K][\mathbb{Q}(\zeta) \cap K : \mathbb{Q}]}{[K(\zeta) : K]} = [\mathbb{Q}(\zeta) \cap K : \mathbb{Q}].$$

We have fixed an a coprime to n. We know there exists $\sigma_a \in G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that $\sigma_a(\zeta) = \zeta^a$.
As G is abelian (it is $\cong (\mathbb{Z}/n\mathbb{Z})^\times$), H is normal in G. This means that $[G : H] = t$ is the order of the group G/H. By Lagrange's Theorem we must have $\sigma_a^t = \sigma_{a^t} \in H = \mathrm{Gal}(K(\zeta)/K)$. □

Lemma 6.2.2. *Let K a number field and $\zeta \in \mu_\infty$ of order n and $\zeta = \eta^k \xi^l$ with $k, l \in \mathbb{Z}$ where $\eta, \xi \in \mu_\infty \cap \mathbb{Q}(\zeta)$. Then we have*

$$\#\{\tau(\eta) : \tau \in \mathrm{Gal}(K(\zeta)/K)\} \geq (\varphi(n)/[K : \mathbb{Q}])^{1/2}$$

or

$$\#\{\tau(\xi) : \tau \in \mathrm{Gal}(K(\zeta)/K)\} \geq (\varphi(n)/[K : \mathbb{Q}])^{1/2}.$$

Proof. We clearly have $[K(\zeta):K] \geq [\mathbb{Q}(\zeta):\mathbb{Q}]/[K:\mathbb{Q}]$, which implies $\#\mathrm{Gal}(K(\zeta)/K) \geq \varphi(n)/[K:\mathbb{Q}]$.
Now, If both of the above inequalities were false we would have $< \varphi(n)/[K:\mathbb{Q}]$ possibilities for $\tau(\zeta) = \tau(\eta)^k\tau(\xi)^l$ as τ varies in $\mathrm{Gal}(K(\zeta)/K)$. This gives a contradiction. □

Exercise 6.2.3. Show that $\varphi(n) = n\prod_{p|n}(1-1/p)$

Lemma 6.2.4. *For any $n \in \mathbb{N}^{>0}$ we have $\varphi(n) \geq (n/2)^{1/2}$.*

Proof. The inequality is true for $n = 1, 2$. Assume $n \geq 3$. We have $t(1-1/t)^2 = t - 2 + 1/t \geq 1$ for all $t \geq 3$ and therefore $t^{1/2}(1-1/t) \geq 1$.
By the exercise above we have

$$\varphi(n) = n^{1/2}\prod_{p|n} p^{\nu_p(n)/2}(1-1/p) \geq n^{1/2}\begin{cases} 1 & : 2 \nmid n, \\ \frac{1}{2}2^{\nu_2(n)/2} \geq \frac{1}{\sqrt{2}} & : 2 \mid n \end{cases}$$

since $p^{\nu_p(n)/2}(1-1/p) \geq 1$ in case $p \geq 3$. □

6.3 Construction of the auxiliary prime number

In this section we prove that, given an integer n there exists a prime number p that does not divide n and is "small".
Let us start with the following lemma.

Lemma 6.3.1. *A natural number $n \geq 0$ has at most $(\log n)/(\log 2)$ prime divisors.*

Proof. We may suppose $n \geq 2$. Let $p_1^{e_1}\cdots p_g^{e_g}$ be the prime factorization of n. We have $p_i \geq 2$ for all i, therefore $n \geq 2^{e_1+\cdots+e_g} \geq 2^g$ and thus $g \leq (\log n)/(\log 2)$. □

We now must count prime numbers. For $x \in \mathbb{R}$ we let

$$\pi(x) = \#\{p \leq x : p \text{ is a prime number}\}.$$

We know since Euclid's times that $\pi(x) \to \infty$ for $x \to \infty$. Chebyshev showed the following.

Theorem 6.3.2. *For $n \in \mathbb{N}$ we have $\pi(2n) \geq \frac{n\log 2}{\log(2n)}$.*

Before we prove this theorem we deduce the following corollary that we are going to use later.
In what follows $\lfloor\cdot\rfloor$ indicates the floor function, also called integral part.

Corollary 6.3.3. *There exists a constant $C > 0$ such that, for every integer $n \geq 2$, there exists a prime number p with $p \nmid n$ and $p \leq C(\log n)^2$.*

Proof. For the integer $m = \left\lfloor \frac{C}{2}(\log n)^2 \right\rfloor$, with $C > 0$ an absolute large enough constant, we have $\pi(2m) > (\log n)/(\log 2)$ by Theorem 6.3.2. By Lemma 6.3.1 there exists a prime number $p \leq 2m \leq C(\log n)^2$ that does not divide n. □

For Theorem 6.3.2 be need the following elementary lemma about the factorization of $n!$ for $n \in \mathbb{N}$.

Lemma 6.3.4. *Let $n \in \mathbb{N}$ and p a prime number. Then we have $\nu_p(n!) = \sum_{e\geq 1} \lfloor n/p^e \rfloor$.*

Note that the sum over e is finite, since $\lfloor n/p^e \rfloor = 0$ for all e with $p^e > n$.

Proof. By definition we have

$$\nu_p(n!) = \sum_{k=1}^{n} \nu_p(k) = \sum_{e\geq 1} \sum_{\substack{k=1 \\ \nu_p(k)=e}}^{n} e = \sum_{e\geq 1} \left(\left\lfloor \frac{n}{p^e} \right\rfloor - \left\lfloor \frac{n}{p^{e+1}} \right\rfloor \right) e,$$

since there are exactly $\lfloor n/p^e \rfloor$ integers $k \in \{1, \ldots, n\}$ which are divisible by p^e. Note that

$$\left(\left\lfloor \frac{n}{p^e} \right\rfloor - \left\lfloor \frac{n}{p^{e+1}} \right\rfloor \right) e = \left\lfloor \frac{n}{p^e} \right\rfloor e - \left\lfloor \frac{n}{p^{e+1}} \right\rfloor (e+1) + \left\lfloor \frac{n}{p^{e+1}} \right\rfloor.$$

Now we write

$$\begin{aligned} \nu_p(n!) &= \sum_{e\geq 1} \left(\left\lfloor \frac{n}{p^e} \right\rfloor e - \left\lfloor \frac{n}{p^{e+1}} \right\rfloor (e+1) + \left\lfloor \frac{n}{p^{e+1}} \right\rfloor \right) \\ &= \left\lfloor \frac{n}{p} \right\rfloor + \sum_{e\geq 1} \left(- \left\lfloor \frac{n}{p^{e+1}} \right\rfloor (e+1) + \left\lfloor \frac{n}{p^{e+1}} \right\rfloor + \left\lfloor \frac{n}{p^{e+1}} \right\rfloor (e+1) \right), \end{aligned}$$

and the claim follows easily. □

Proof of Theorem 6.3.2. Consider the binomial coefficient $A_n = \binom{2n}{n} = (2n!)/(n!)^2$. For a prime number p, Lemma 6.3.4 implies that

$$\nu_p(A_n) = \sum_{\substack{e\geq 1 \\ p^e \leq 2n}} \left(\left\lfloor \frac{2n}{p^e} \right\rfloor - 2 \left\lfloor \frac{n}{p^e} \right\rfloor \right).$$

But $\lfloor 2x \rfloor - 2\lfloor x \rfloor < 2x - 2(x-1) = 2$ and therefore the difference in the sum above is at most 1. We then have

$$\nu_p(A_n) \leq \sum_{\substack{e\geq 1 \\ p^e \leq 2n}} 1 \leq \frac{\log(2n)}{\log p},$$

which implies $p^{\nu_p(A_n)} \leq 2n$.
But $A_n = \prod_p p^{\nu_p(A_n)}$ and every prime divisor p of A_n satisfies $p \leq 2n$. Thus, there are at most $\pi(2n)$ prime divisors of A_n and we obtain

$$A_n \leq (2n)^{\pi(2n)}. \tag{6.1}$$

On the other hand we may simplify $n!$ in A_n and get

$$A_n = \frac{(2n)!}{(n!)^2} = \frac{2n}{n} \frac{2n-1}{n-1} \cdots \frac{n+1}{1}.$$

For $0 \leq k < n$ we have $(2n-k)/(n-k) \geq 2$. Thus, $A_n \geq 2^n$.
If we compare this with (6.1) we see that

$$\pi(2n) \geq \frac{n \log 2}{\log(2n)}. \qquad \square$$

6.4 Proof of the Theorem of Ihara, Serre and Tate

We need the following lemma.

Lemma 6.4.1. *Let $P \in \overline{\mathbb{Q}}[X,Y] \setminus \overline{\mathbb{Q}}$ be irreducible and not a monomial. Let p be a prime number and $t \in \mathbb{N}$, $t > 0$, so that $P \mid P(X^{p^t}, Y^{p^t})$. If $p > 2(\deg P)^2$, there exist $\alpha, \beta \in \overline{\mathbb{Q}}^\times$ and $(r,s) \in \mathbb{Z}^2 \setminus \{0\}$ with $r \geq 0, s \geq 0$ and $P = \alpha X^r Y^s - \beta$ or $P = \alpha X^r - \beta Y^s$.*

Proof. We write $q = p^t$. We have $P(X^q, Y^q) = PS$ for some $S \in \overline{\mathbb{Q}}[X,Y]$.
Let $G = \{(\eta, \xi) \in \overline{\mathbb{Q}}^2 : \eta^q = \xi^q = 1\}$. This is a subgroup of $(\overline{\mathbb{Q}}^\times)^2$ of order $p^{2t} = q^2$.
For all $g = (\eta, \xi) \in G$ by substituting $(X,Y) \mapsto (\eta X, \xi Y)$ we get the equality $P(X^q, Y^q) = P(\eta X, \xi Y) S(\eta X, \xi Y)$. The polynomial $P_g = P(\eta X, \xi Y) \in \overline{\mathbb{Q}}[X,Y]$ is still a divisor of $P(X^q, Y^q)$. Moreover, P_g is irreducible as an element of $\overline{\mathbb{Q}}[X,Y]$, as the transformation $(X,Y) \mapsto (\eta X, \xi Y)$ is linear.
Now we want to find out how many of the P_g are coprime to each other.
Suppose all P_g for $g \in G$ are pairwise coprime. As the P_g are all irreducible we must have that $\prod_{g \in G} P_g$ divides $P(X^q, Y^q)$. Therefore,

$$q^2 \deg P = \#G \deg P \leq \deg P(X^q, Y^q) = q \deg P,$$

a contradiction.
We deduce that there are distinct $(\eta_1, \xi_1), (\eta_2, \xi_2) \in G$, such that $P_{(\eta_1,\xi_1)}$ and $P_{(\eta_2,\xi_2)}$ have a common divisor. Since they are both irreducible, we must have $P(\eta_1 X, \xi_1 Y) = \lambda P(\eta_2 X, \xi_2 Y)$ for a $\lambda \in \overline{\mathbb{Q}}^\times$. We now write $P = \sum_{i,j} a_{ij} X^i Y^j$ and compare coefficients. We have $a_{ij} \eta_1^i \xi_1^j = \lambda a_{ij} \eta_2{}^i \xi_2{}^j$ for all i, j. Therefore, $(\eta_1/\eta_2)^i (\xi_1/\xi_2)^j = \lambda$ for all (i,j) with $a_{ij} \neq 0$.
We obtain that there is $(\eta, \xi) \in G \setminus \{(1,1)\}$ such that $\eta^i \xi^j = \lambda$ for all (i,j) with $a_{ij} \neq 0$.
The support $\operatorname{supp} P$ of P is the finite set $\{(i,j) \in \mathbb{Z}^2 : a_{ij} \neq 0\}$. Let $(i_0, j_0) \in \operatorname{supp} P$ be a fixed point of the support of P. We write $\eta = e^{2\pi\sqrt{-1}a/q}$ and $\xi = e^{2\pi\sqrt{-1}b/q}$ with $a, b \in \{0, \ldots, q-1\}$ not both 0.
For all $(i,j) \in \operatorname{supp} P$ we have $\eta^{i-i_0} \xi^{j-j_0} = 1$, and thus $a(i-i_0) + b(j-j_0) \equiv 0 \pmod q$.
Therefore, the coset $(\overline{a}, \overline{b}) = (a,b) + q\mathbb{Z}^2 \in (\mathbb{Z}/q\mathbb{Z})^2 \setminus \{0\}$ satisfies the system of linear equations given by

$$\overline{a}(i - i_0) + \overline{b}(j - j_0) = 0 \text{ in } \mathbb{Z}/q\mathbb{Z} \text{ for all } (i,j) \in \operatorname{supp} P.$$

The number of equations is $\#\operatorname{supp} P$, an equation for each pair $(i,j) \in \operatorname{supp} P$. Let $(i,j), (i',j') \in \operatorname{supp} P$. As the solution $(\overline{a}, \overline{b})$ is not trivial, we have that

$$\begin{pmatrix} i - i_0 & j - j_0 \\ i' - i_0 & j' - j_0 \end{pmatrix}$$

is not invertible modulo q. It follows that its determinant is divisible by p. The absolute value of this determinant is at most $|i-i_0||j'-j_0|+|j-j_0||i'-i_0| \leq 2(\deg P)^2$. By hypothesis we have $p > 2(\deg P)^2$ and therefore this determinant must vanish.
Therefore, all $(i,j)-(i_0,j_0)$ with $(i,j) \in \operatorname{supp} P$ must lie on a line passing through the origin. This means that $\operatorname{supp} P-(i_0,j_0)$ lies in a subgroup of $\mathbb{Z}^2$ of rank 1. By the structure theorem of finitely generated abelian groups, this subgroup must have a basis $(v,w) \in \mathbb{Z}^2 \setminus \{0\}$. Therefore $\operatorname{supp} P \subset (i_0,j_0)+(v,w)\mathbb{Z}$. As (i_0,j_0) was arbitrary, we might chose it so that any element of $\operatorname{supp} P$ is of the form $(i_0+v\mu, j_0+w\mu)$ with $\mu \geq 0$ in $\mathbb{Z}$.
Then, there exists $R \in \overline{\mathbb{Q}}[T]$ with $P = X^{i_0}Y^{j_0}R(X^vY^w)$. Over $\overline{\mathbb{Q}}$ the polynomial R splits in linear factors. But we have that P is irreducible and has at least two terms. It follows that R is of the form $\alpha T+\beta$ with $\alpha,\beta \in \overline{\mathbb{Q}}^\times$. The lemma now follows as P is not a multiple X or Y. □

The following generalises Theorem 6.1.1.

Theorem 6.4.2 (Ihara, Serre, Tate)**.** *Let $K \subseteq \mathbb{C}$ be a number field and $P \in K[X,Y]$ be an irreducible polynomial such that $\{(\eta,\xi) \in \mu_\infty : P(\eta,\xi)=0\}$ is infinite. Then, there exist integers $r,s \geq 0$, not both zero, such that P divides X^rY^s-1 or X^r-Y^s.*

Proof. We start by showing that we may relax the condition on the irreducibility of P in $K[X,Y]$ and just assume irreducibility in $\overline{\mathbb{Q}}[X,Y]$.
Suppose we have proved the theorem with this weaker hypothesis.
Our polynomial P factors over $\overline{\mathbb{Q}}[X,Y]$ in finitely many irreducible factors. For one of these factors, say $Q \in \overline{\mathbb{Q}}[X,Y]$, we have $Q(\eta,\xi)=0$ for infinitely many $(\eta,\xi) \in \mu_\infty^2$.
Then, Q divides some G of the form X^rY^s-1 or X^r-Y^s. The set of common roots in $\overline{\mathbb{Q}}$ of P and G is then infinite and recall that P is irreducible over K. Then, Lemma 4.2.5 implies that P divides G.
We may then assume that P is irreducible in $\overline{\mathbb{Q}}[X,Y]$.
Let $\eta,\xi \in \mu_\infty$ with $P(\eta,\xi)=0$. Let η be of order r and ξ of order s. The set

$$\{\eta^a\xi^b : a,b \in \mathbb{Z}\} = \{\eta^k\xi^l : k \in \{1,\dots,r\} \text{ and } l \in \{1,\dots,s\}\}$$

is a finite subgroup of $\mathbb{C}^\times$, and therefore cyclic. Therefore there is $\zeta \in \mu_\infty$ with $\eta=\zeta^k$ and $\xi=\zeta^l$ for some $k,l \in \mathbb{Z}$. We have $P(\zeta^k,\zeta^l)=0$. Let n be the order of ζ.
By Corollary 6.3.3 there exists a prime number $p \nmid n$ with $p \leq c_1(\log n)^2$, where $c_1>0$ is an absolute constant. We set $c_2 = (2(\deg P)^2)!$. The same corollary applied to $c_2 n$, produces a $p \nmid n$,

$$p \leq c_1(\log(c_2 n))^2 \tag{6.2}$$

and $p \nmid c_2$. This last property and the definition of c_2 tells us that $p > 2(\deg P)^2$.
We use Proposition 6.2.1 with $a=p$ and get a $\sigma \in \operatorname{Gal}(K(\zeta)/K)$ with $\sigma(\zeta)=\zeta^{p^t}$ for some $t \leq [K:\mathbb{Q}]$. As $\eta=\zeta^k$ we have $\sigma(\eta)=\eta^{p^t}$ and analogously $\sigma(\xi)=\xi^{p^t}$. Since (η,ξ) is a root of P and σ fixes the coefficients of P, we conclude that

$$0 = \sigma(P(\eta,\xi)) = P(\sigma(\eta),\sigma(\xi)) = P(\eta^{p^t},\xi^{p^t}).$$

For every other automorphism $\tau \in \mathrm{Gal}(K(\zeta)/K)$, we have that $(\tau(\eta), \tau(\xi))$ is a common root of P and of $P(X^{p^t}, Y^{p^t})$.
Applying Lemmas 6.2.2 and 6.2.4 and by symmetry, we may assume that the number of conjugates $\tau(\eta)$ is at least $(\varphi(n)/[K:\mathbb{Q}])^{1/2} \geq n^{1/4}/(2^{1/4}[K:\mathbb{Q}]^{1/2})$. We now consider P and $P(X^{p^t}, Y^{p^t})$ as polynomials in Y and denote their resultant with R. Note that the claim of the theorem is trivial if P or $P(X^{p^t}, Y^{p^t})$ do not depend on Y.
There are two cases:

Case 1. $R = 0$.
By Corollary 4.2.6 and as P is irreducible, it follows that $P \mid P(X^{p^t}, Y^{p^t})$. By Lemma 6.4.1 we have $P = \alpha X^r Y^s - \beta$ or $P = \alpha X^r - \beta Y^s$ for some $\alpha, \beta \in \overline{\mathbb{Q}}^\times$. Since P has a root of the form $(\eta, \xi) \in \mu_\infty^2$, we have $\beta/\alpha = \epsilon \in \mu_\infty$. It follows that P is equal to $X^r Y^s - \epsilon$ or $X^r - \epsilon Y^s$ up to multiplying by a scalar. Let $m = \operatorname{ord} \epsilon$. If $P = X^r Y^s - \epsilon$ than P divides the polynomial

$$\prod_{j=1}^{m} (X^r Y^s - \epsilon^j) = X^{rm} Y^{sm} - 1.$$

The case $P = X^r - \epsilon Y^s$ can be dealt with similarly. We are then done with Case 1.

Case 2. $R \neq 0$.
We use Lemma 4.2.4 and get two polynomials $A, B \in K[X, Y]$ such that $R = AP + BP(X^{p^t}, Y^{p^t})$. We let $c_3 = \max\{\deg_X A, \deg_X B\}$. This is a constant independent of n. Then

$$\begin{aligned} \deg R &\leq c_3(\deg_X P + \deg_X P(X^{p^t}, Y^{p^t})) \\ &\leq c_3(\deg P + p^t \deg P) \leq c_3 \deg(P)(c_1(\log(c_2 n))^2)^{[K:\mathbb{Q}]}. \end{aligned}$$

where we have used the bound (6.2) and $t \leq [K:\mathbb{Q}]$.
We now note that $R(\tau(\eta)) = 0$ for all $\tau \in \mathrm{Gal}(K(\zeta)/K)$. This implies that

$$\deg R \geq \frac{n^{1/4}}{2^{1/4}[K:\mathbb{Q}]^{1/2}}.$$

Combining these upper and lower bounds for $\deg R$ we obtain

$$\frac{n^{1/4}}{2^{1/4}[K:\mathbb{Q}]^{1/2}} \leq c_3 \deg(P)(c_1(\log(c_2 n))^2)^{[K:\mathbb{Q}]}.$$

For n sufficiently large this inequality gives a contradiction. This means that this case 2 gives a bound for n in terms of P. Therefore there are at most finitely many possibilities for the pair (η, ξ). □

7 Thue's Theorem

7.1 Introduction

The following theorem was the prelude to many important advances in number theory in the 20th century. It dates back to Thue.

Theorem 7.1.1. *Let $F \in \mathbb{Q}[X,Y]$ be a homogeneous irreducible polynomial of degree at least 3. For every rational number $k \in \mathbb{Q} \setminus \{0\}$ the set*

$$\{(x,y) \in \mathbb{Z}^2 : F(x,y) = k\}$$

is finite.

Example 7.1.2. There are at most finitely many $(x,y) \in \mathbb{Z}^2$ with $x^3 - 2y^3 = 1$. Among these solutions we have $(x,y) = (-1,-1)$ and $(x,y) = (1,0)$.

Theorem 7.1.1 is mainly known because of the proof method it introduced. We will get to know it in more detail below. At the center of this method lies a question of *Diophantine approximation*: How well can one approximate an algebraic number by a rational number? Of course, any real number can be approximated arbitrarily well using rational numbers. Diophantine approximation deals with the most efficient approximations possible.

Example 7.1.3. Let $x^3 - 2y^3 = 1$ with $x, y \in \mathbb{Z}$. Assume that $y \neq 0$. Then, $(x/y)^3 - 2 = 1/y^3$ and thus

$$\left(\frac{x}{y} - 2^{1/3}\right)\left(\frac{x}{y} - 2^{1/3}\zeta\right)\left(\frac{x}{y} - 2^{1/3}\zeta^2\right) = \frac{1}{y^3}$$

where $\zeta = e^{2\pi\sqrt{-1}/3}$. If we consider the imaginary part we see that $|x/y - 2^{1/3}\zeta| \geq \mathrm{Im}(2^{1/3}\zeta) > 1$. The same holds for ζ^2 in place of ζ. It follows that $|x/y - 2^{1/3}| \leq 1/y^3$. We prove Theorem 7.1.1 by contradiction. So we assume that the there are infinitely many $(x,y) \in \mathbb{Z}^2$ with $x^3 - 2y^3 = 1$. The above considerations imply that the inequality

$$\left|\frac{x}{y} - 2^{1/3}\right| \leq \frac{1}{y^3} \tag{7.1}$$

has infinitely many solutions $(x,y) \in \mathbb{Z}^2$ with $x \neq 0$. We are going to see later that this is impossible.

With the theory of heights we can find a simple lower bound for $|x/y - \alpha|$. The following estimate is attributed to Liouville.

Theorem 7.1.4 (Liouville). *Let $\alpha \in \mathbb{C}$ be an algebraic number with $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $x, y \in \mathbb{Z}$ with $y \geq 1$. If $\alpha \neq x/y$, we have*

$$\left|\alpha - \frac{x}{y}\right| \geq \frac{1}{2^d H(\alpha)^d H(x/y)^d} \quad \text{and} \quad \left|\alpha - \frac{x}{y}\right| \geq \frac{1}{2^d (1+|\alpha|)^d H(\alpha)^d y^d}. \tag{7.2}$$

Proof. For all algebraic numbers $\beta \in \mathbb{C}^\times$ we have $H(\beta^{-1}) = H(\beta)$ by Lemma 3.3.3. We recall that by definition we have

$$H(\beta)^{[\mathbb{Q}(\beta):\mathbb{Q}]} = H(\beta^{-1})^{[\mathbb{Q}(\beta):\mathbb{Q}]} = \prod_{v \in M(\mathbb{Q}(\beta))} \max\{1, |\beta^{-1}|_v\}^{d_v}.$$

All factors are ≥ 1 and among the factors we have $\max\{1, |\beta^{-1}|\}$. It follows that $H(\beta)^{[\mathbb{Q}(\beta):\mathbb{Q}]} \geq \max\{1, |\beta^{-1}|\} \geq 1/|\beta|$ which implies $|\beta| \geq 1/H(\beta)^{[\mathbb{Q}(\beta):\mathbb{Q}]}$.
We apply the last inequality to $\beta = \alpha - x/y \neq 0$. By Lemma 3.3.6 and $H(x/y) = H(-x/y)$ we have $H(\beta) \leq 2H(\alpha)H(x/y)$. This gives the first inequality of (7.2).
For the second we may assume $|\alpha - x/y| \leq 1$. By $|y\alpha - x| \leq y$ we get $|x| \leq y(1+|\alpha|)$ using the triangular inequality and, as $H(x/y) \leq \max\{|x|, y\}$, we have $H(x/y) \leq (1+|\alpha|)y$ and we are done with the theorem. □

Remark 7.1.5.

(i) Liouville's Theorem is not strong enough to deduce Theorem 7.1.1. In the above example with $\alpha = 2^{1/3}$ and $d = [\mathbb{Q}(2^{1/3}) : \mathbb{Q}] = 3$ we get the inequality $|2^{1/3} - x/y| \geq 2^{-3}(1+2^{1/3})^{-3} H(2^{1/3})^{-3} y^{-3} > 1/(185y^3)$. This does not contradict the assumption that (7.1) has infinitely many solutions x and y.

(ii) If only it was possible in the example $\alpha = 2^{1/3}$ to improve the expontent, $d = 3$ of y to 2.9999999999999999, we could conclude that so $x^3 - 2y^3 = 1$ has at most finitely many solutions. This would also be the case, with a possibly different constant in the place of $2^{-d}(1+|\alpha|)^{-d} H(\alpha)^{-d}$.

Theorem 7.1.6 (Thue 1909). *Let $\alpha \in \mathbb{C}$ be an algebraic number $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. For all $\epsilon > 0$ there is a constant $C(\alpha, \epsilon) > 0$, such that*

$$\left|\alpha - \frac{x}{y}\right| \geq \frac{C(\alpha, \epsilon)}{|y|^{d/2+1+\epsilon}}$$

for all $x, y \in \mathbb{Z}$ with $y \neq 0$ and $x/y \neq \alpha$.

The proof will keep us busy for a while. Roughly speaking, the underlying idea has already appeared in a simplified form in the proof of Theorem 4.3.2. We will construct an auxiliary function, but this time the linear algebra from Lemma 4.3.5 is not sufficient, instead we will use the Pidgeon-hole Principle to construct an auxiliary polynomial.
If we assume Thue's theorem, the proof of Theorem 7.1.1 is simple.

Proof of Theorem 7.1.1 assuming Theorem 7.1.6. The polynomial F is homogeneous, irreducible and has degree $d \geq 3$. In particular, $X \nmid F$ and $Y \nmid F$. The de-homogenised polynomial $F(X, 1)$ has also degree d and factors $F(X, 1) = f(X - \alpha_1) \cdots (X - \alpha_d)$,

where α_i are algebraic numbers in $\mathbb{C}$ with $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = d$ for all $i \in \{1, \dots, d\}$ and $f \in \mathbb{Q}^\times$. Homogenizing again we get $F(X, Y) = f \prod_{i=1}^{d} (X - \alpha_i Y)$.
Fix a solution $(x, y) \in \mathbb{Z}^2$. The polynomial $F(X, 0) - k$ has at most finitely many roots so we may assume $y \neq 0$.
We let $\eta = \min_{i \neq j} |\alpha_i - \alpha_j|$. This cannot be zero by the irreducibility of F.
Now we choose $i_0 \in \{1, \dots, d\}$ such that $\varphi := |x - \alpha_{i_0} y| \leq |x - \alpha_i y|$ for all $i \in \{1, \dots, d\}$.
We consider two cases.
Case 1. $\varphi < \eta|y|/2$. Then,

$$\frac{|k|}{|f|} = \prod_{i=1}^{d} |x - \alpha_i y| \geq \varphi \prod_{i \neq i_0} (|\alpha_i - \alpha_{i_0}||y| - |x - \alpha_{i_0} y|) \geq \varphi \prod_{i \neq i_0} (\eta|y| - \varphi) > \varphi \left(\frac{\eta|y|}{2}\right)^{d-1}.$$

This implies

$$\left|\alpha_{i_0} - \frac{x}{y}\right| \leq \frac{|k|}{|f|} \left(\frac{2}{\eta}\right)^{d-1} \frac{1}{|y|^d}. \tag{7.3}$$

Case 2. $\varphi \geq \eta|y|/2$. Then,

$$\varphi \left(\frac{\eta|y|}{2}\right)^{d-1} \leq \varphi^d \leq \prod_{i=1}^{d} |x - \alpha_i y| = \frac{|k|}{|f|},$$

and this implies (7.3), as well.
On the other hand Thue's Theorem with $\epsilon = 1/4$ gives the inequality $|\alpha_{i_0} - x/y| \geq C(\alpha_{i_0}, 1/4)|y|^{-(d/2+1+1/4)}$ for some constant $C(\alpha_{i_0}, 1/4) > 0$.
We compare upper and lower bounds and get

$$\frac{C(\alpha_{i_0}, 1/4)}{|y|^{d/2+5/4}} \leq \left|\alpha_{i_0} - \frac{x}{y}\right| \leq \left|\frac{k}{f}\right| \left(\frac{2}{\eta}\right)^{d-1} \frac{1}{|y^d|}.$$

It follows that, for any solution $(x, y) \in \mathbb{Z}^2$ we have $|y|^{1/4} = |y|^{3/2-5/4} \leq |y|^{d/2-5/4} \leq \max_{1 \leq i \leq d}\{|k| 2^{d-1}/(C(\alpha_i, 1/4)|f|\eta^{d-1})\}$ which implies that $|y|$ is bounded.
There are then at most finitely many $y \in \mathbb{Z}$ with $F(x, y) = k$ for some $x \in \mathbb{Z}$. But for all $y \in \mathbb{Z}$ there are at most d distinct x with $F(x, y) = k$. Therefore there are at most finitely many $(x, y) \in \mathbb{Z}^2$ with $F(x, y) = k$. □

Remark 7.1.7. Thue's Theorem implies that we may replace the exponent d of y^d in Liouville's Theorem by $1 + d/2 + \epsilon$, up to changing the constant.
Let α be an algebraic number. For which real $\kappa > 0$ there exists $C = C(\alpha, \kappa) > 0$ such that

$$\left|\alpha - \frac{x}{y}\right| \geq \frac{C}{y^\kappa} \tag{7.4}$$

for all $x, y \in \mathbb{Z}$ and $y \geq 1$ and $x/y \neq \alpha$?
The smaller κ, the stronger the conclusion.
Liouville's Theorem implies that $\kappa = [\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ is possible.
Thue says that any $\kappa > 1 + d/2$ works.
What is the optimal κ? In other word, what is the liminf of the possible κ as a function of α?

(i) The case $d = 1$, i.e., $\alpha \in \mathbb{Q}$, is trivial. Here $\alpha = p/q$ with $p, q \in \mathbb{Z}$ and $q \geq 1$. Let $x, y \in \mathbb{Z}$ with $y \geq 1$. For $\alpha = p/q \in \mathbb{Q}$ with $q \geq 1$ and $\alpha \neq x/y$ we have

$$\left|\frac{p}{q} - \frac{x}{y}\right| = \frac{|py - qx|}{qy} \geq \frac{1}{qy},$$

as $py - qx \in \mathbb{Z} \setminus \{0\}$. In case $\alpha \in \mathbb{Q}$ the exponent $\kappa = 1$ works. This is better than Liouville's and Thue's Theorem, but it is trivial.

(ii) For $d = 2$ Liouville gives the exponent $\kappa = 2$ while Thue gives any $\kappa > 2$. In this special case Liouville is still better than Thue.

(iii) For $d \geq 3$ we have $1 + d/2 < d$ and thus Thue is quite stronger than Liouville.

(iv) In 1921 Siegel proved that one can take $\kappa = 2\sqrt{d}$. Dyson improved this to $\kappa = \sqrt{2d}$. The last step was proven by Roth in 1955. He showed that we can take $\kappa = 2 + \epsilon$ for any $\epsilon > 0$. Roth received the Fields Medal because of this result, among other things.

(v) The proof of Thue's Theorem is **ineffective**. This means that the proof does not give us any way of determining the constant $C(\alpha, \epsilon)$. By the theorem it follows that $|2^{1/3} - x/y| \geq C|y|^{-2.5000000001}$ for a constant $C > 0$. Nobody knows such constant!
With a completely different method, Alan Baker showed that $|2^{1/3} - x/y| \geq 10^{-6}/y^{2.955}$ for all $x, y \in \mathbb{Z}$ with $y \geq 1$. The exponent 2.955 is very close but still strictly smaller than 3. Therefore Baker's estimate is sufficient to solve the Diophantine equation $x^3 - 2y^3 = 1$, cfr. Remark 7.1.5(ii).

We now show that we must have $\kappa \geq 2$ for all irrational $\alpha \in \mathbb{R}$.

Theorem 7.1.8 (Dirichlet)**.** *Let $\alpha \in \mathbb{R}$ and $Q > 0$ in $\mathbb{Z}$. There exist $p, q \in \mathbb{Z}$ with $\gcd(p, q) = 1$, such that*

$$1 \leq q \leq Q, \qquad \left|\alpha - \frac{p}{q}\right| \leq \frac{1}{q(Q+1)}. \tag{7.5}$$

Proof. We first show that there are not necessarily coprime p, q that fulfill (7.5).
We consider the sequence of the $Q + 1$ real numbers $0, \{\alpha\}, \{2\alpha\} \ldots, \{Q\alpha\}$ which lie in $[0, 1)$. Here $\{x\} = x - \lfloor x \rfloor$ indicates the fractional part of the real number x.
If we divide the interval $[0, 1)$ in the $Q + 1$ subintervals $\left[\frac{j}{Q+1}, \frac{j+1}{Q+1}\right), j = 0, \ldots, Q$, it follows from the Pigeonhole principle, that either every subinterval contains exactly one number from the sequence or there is a subinterval that contains two of them.
In the first case there is an integer q with $1 \leq q \leq Q$ and $\frac{Q}{Q+1} \leq \{q\alpha\} < 1$, which means $\frac{Q}{Q+1} \leq q\alpha - \lfloor q\alpha \rfloor < 1$. Then, this q and $p = \lfloor q\alpha \rfloor + 1$ fulfil the inequalities (7.5).
In the second case, there are two integers r, s with $0 \leq s < r \leq Q$ and $|\{r\alpha\} - \{s\alpha\}| < \frac{1}{Q+1}$. Then the inequalities (7.5) are fulfilled by $p = \lfloor r\alpha \rfloor - \lfloor s\alpha \rfloor$ and $q = r - s$.
Finally, if p and q are not coprime, we can divide them both by $\gcd(p, q)$. The two inequalities (7.5) still hold. □

Corollary 7.1.9. *Let $\alpha \in \mathbb{R}$. There are infinitely many pairs $(p, q) \in \mathbb{Z}^2$, $q \geq 1$, with*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2} \tag{7.6}$$

if and only if $\alpha \notin \mathbb{Q}$.

Proof. Suppose α is irrational. We choose an integer $Q = Q_1 > 0$. By Dirichlet's Theorem we get a pair (p_1, q_1) with

$$\delta_1 := \left|\alpha - \frac{p_1}{q_1}\right| \leq \frac{1}{q_1(Q_1 + 1)} < \frac{1}{q_1^2}.$$

Since α is irrational we have that δ_1 is positive and we let $Q_2 > 1/\delta_1$ be a new integer. We apply Dirichlet's Theorem again and get p_2, q_2 with

$$\delta_2 := \left|\alpha - \frac{p_2}{q_2}\right| < \frac{1}{q_2^2},$$

but

$$\left|\alpha - \frac{p_2}{q_2}\right| < \frac{1}{q_2(Q_2 + 1)} < \frac{1}{Q_2} < \delta_1 = \left|\alpha - \frac{p_1}{q_1}\right|$$

so $\frac{p_2}{q_2} \neq \frac{p_1}{q_1}$.
Now we choose again $Q_3 > 1/\delta_2$ and so on. We then construct an infinite sequence of distinct pairs as wanted.
Now, let $\alpha = \frac{a}{b} \in \mathbb{Q}$ a reduced fraction. For all $\frac{p}{q} \in \mathbb{Q}$ we have either $\frac{p}{q} = \frac{a}{b}$, or

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{bq}.$$

Indeed,

$$\left|\alpha - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq},$$

since a positive integer is at least 1! □

This corollary shows that we must have $\kappa \geq 2$ in (7.4) for all irrational numbers α.

Remark 7.1.10. In Theorem 7.1.1, the assumption $d \geq 3$ is necessary. A complete treatment of the case of F of degree 2 can be found at the end of the first chapter of [10]. The prominent example is given by the well-known Pell equation

$$X^2 - DY^2 = 1$$

which has a solution (and therefore infinitely many) $(x, y) \in \mathbb{Z}^2 \setminus \{(1, 0)\}$ if and only if $D > 0$ is not a square in $\mathbb{Z}$.

7.2 Siegel's Lemma

In the proof of Lemma 4.3.5 we constructed an auxiliary polynomial with the help of linear algebra. A more refined construction is necessary for the proof of Thue's theorem. We will solve a linear system of equations with integer coefficients quantitatively. The corresponding result is called "Siegel's Lemma". It is fundamental in Diophantine approximation and transcendence theory.

Definition 7.2.1. Let M and N be positive integers. We indicate by $\|\cdot\|$ the maximum norm on the real vector spaces $\mathrm{M}_{M,N}(\mathbb{R})$ and $\mathbb{R}^M$.

Lemma 7.2.2 (Siegel)**.** *Let M, N be integers with $N > M \geq 1$ and $A \in M_{M,N}(\mathbb{Z})$. Let $B \geq 1$ be a real number with $\|A\| \leq B$. There exists $x \in \mathbb{Z}^N \setminus \{0\}$ with*

$$\|x\| \leq (NB)^{M/(N-M)}$$

such that $Ax = 0$.

Proof. The proof is an application of the Pidgeon-hole Principle
Let $T \geq 0$ be an integer that we are going to fix later. The number of points of $\mathbb{Z}^N \cap [0,T]^N$ is $(1+T)^N$.
We write $A = (a_{ij})_{\substack{1\leq i\leq M\\ 1\leq j\leq N}}$. Let $x \in \mathbb{Z}^N \cap [0,T]^N$ and $y = Ax$ with $y = (y_1, \ldots, y_M)^t$. We have

$$-TN_i \leq y_i \leq TP_i \tag{7.7}$$

where

$$P_i = \sum_{\substack{j=1\\ a_{ij}\geq 0}}^{N} a_{ij} \geq 0 \quad \text{and} \quad N_i = \sum_{\substack{j=1\\ a_{ij}<0}}^{N} -a_{ij} \geq 0$$

for all $i \in \{1, \ldots, M\}$. Note that $P_i + N_i \leq NB$.
For a fixed i the number of possible $y_i \in \mathbb{Z}$ that satisfy (7.7) is equal to $T(P_i+N_i)+1 \leq BNT+1$. We have M coordinates, so for y there are at most $(BNT+1)^M$ possibilities. The number of possibilities for $x \in \mathbb{Z}^N \cap [0,T]^N$ is $(T+1)^N$.
We suppose for the moment that

$$(T+1)^N > (BNT+1)^M \tag{7.8}$$

holds. Then, by the Pidgeon-hole Principle there exist distinct $x', x'' \in \mathbb{Z}^N \cap [0,T]^N$ with $Ax' = Ax''$. It follows that $Ax = 0$ for $x = x' - x''$. Moreover, $\|x\| \leq T$.
We now show that if we choose $T = \lfloor (NB)^{M/(N-M)} \rfloor$ the inequality (7.8) holds and this will prove the lemma.
For all $x \in \mathbb{R}$ we have $\lfloor x \rfloor + 1 > x$. Therefore, $(T+1)^{N-M} > (NB)^M$ and so $(T+1)^N > (T+1)^M (NB)^M = ((T+1)NB)^M = (BNT+NB)^M \geq (BNT+1)^M$. Therefore, (7.8) holds for our choice of T. □

Example 7.2.3. We consider the polynomial $(X-1)^{2020}$. The coefficient of X^{1010} is $\binom{2020}{1010} > 2 \cdot 10^{606}$, so very large. Is there a polynomial $Q \in \mathbb{Z}[X] \setminus \{0\}$ such that all coefficients of $(X-1)^{2020}Q$ lie in $\{0, \pm 1\}$?
Consider the general polynomial $(X-1)^M$ with $M \geq 1$. Any polynomial $P \in \mathbb{Z}[X] \setminus \{0\}$ such that

$$\frac{d^i P}{dX^i}(1) = 0 \quad \text{for all} \quad i \in \{0, \dots, M-1\} \tag{7.9}$$

is going to be a multiple of $(X-1)^M$.
We write $P = \sum_{j=0}^{N-1} a_j X^j$ for some parameter N. Then (7.9) becomes a homogeneous system of M linear equations

$$\sum_{j=0}^{N-1} a_j j(j-1)\cdots(j-i+1) = 0 \quad \text{for all} \quad i \in \{0, \dots, M-1\}$$

with integer coefficients in the unknowns $a_0, \dots, a_{N-1}$. We obtain a matrix $A \in \mathrm{M}_{M,N}(\mathbb{Z})$. The entries of A are non-negative and, since $j^i \leq N^M$, we have $\|A\| \leq N^M$.
We assume $N > M$. By Siegel's Lemma it follows that there is an $x \in \mathbb{Z}^N \setminus \{0\}$ with $Ax = 0$ and $\|x\| \leq (N^{M+1})^{M/(N-M)} = N^{M(M+1)/(N-M)}$. This x gives a polynomial $P \neq 0$, which is a multiple of $(X-1)^M$ and lies in $\mathbb{Z}[X] \setminus \{0\}$.
Now, M is fixed and we have $\lim_{N\to\infty} N^{M(M+1)/(N-M)} = 1$. In particular, for a fixed M there is a large enough $N > M$ with $N^{M(M+1)/(N-M)} < 2$. For this choice of N the polynomial P has coefficients in $\{0, \pm 1\}$.
In the special case $M = 2020$ one can take $N = 109001719$.

7.3 The auxiliary polynomial

In this section we construct a polynomial that we are going to use in the proof of Thue's Theorem.
We start with an easy lemma.

Lemma 7.3.1. *Let α be an algebraic integer of degree $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. There exists $c_1(\alpha) > 1$ with the following property. For all $i \geq 0$ there are integers $a_{i0}, \dots, a_{i,d-1} \in \mathbb{Z}$ with $|a_{ij}| \leq c_1(\alpha)^i$ for all $j \in \{0, \dots, d-1\}$ and $\alpha^i = \sum_{j=0}^{d-1} a_{ij}\alpha^j$.*

Proof. We know there is $A = X^d + a_1 X^{d-1} + \cdots + a_d \in \mathbb{Z}[X] \setminus \{0\}$ with $A(\alpha) = 0$. We set $c_1 = 2\max\{|a_1|, \dots, |a_d|\} \geq 2$.
We construct the a_{ij} by induction on i. The case $0 \leq i < d$ is trivial. Let $i \geq d$.
We have $\alpha^i = \alpha^{i-1}\alpha = \sum_{j=0}^{d-1} a_{i-1,j}\alpha^{j+1} = (\sum_{j=1}^{d-1} a_{i-1,j-1}\alpha^j) + a_{i-1,d-1}\alpha^d$. We use $A(\alpha) = 0$ and find $\alpha^d = -a_1\alpha^{d-1} - \cdots - a_d$. Therefore,

$$\alpha^i = \left(\sum_{j=1}^{d-1} a_{i-1,j-1}\alpha^j\right) - \sum_{j=0}^{d-1} a_{i-1,d-1}a_{d-j}\alpha^j = -a_{i-1,d-1}a_d + \sum_{j=1}^{d-1}(a_{i-1,j-1} - a_{i-1,d-1}a_{d-j})\alpha^j.$$

We set $a_{ij} = a_{i-1,j-1} - a_{i-1,d-1}a_{d-j}$ for $j \in \{1, \dots, d-1\}$ and $a_{i,0} = -a_{i-1,d-1}a_d$.

By the inductive hypothesis $|a_{i-1,j}| \le c_1(\alpha)^{i-1}$ and it follows that

$$|a_{ij}| \le 2c_1(\alpha)^{i-1} \max_k |a_k| \le c_1(\alpha)^i$$

using the definition of $c_1(\alpha)$. □

Now we can construct the polynomial we are looking for. We introduce parameters D, m, δ for this.
A polynomial $P = p_0X^D + \cdots + p_D \in \mathbb{R}[X]$ of degree at most D can be seen as a vector $(p_0, \ldots, p_D) \in \mathbb{R}^{D+1}$. We write $\|P\|$ for the maximum norm of this vector.

Proposition 7.3.2. *Let $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ be an algebraic integer with $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. Let $D \ge 1$ and $m \ge 1$ be integers and $\delta \in (0, 1/2]$ with*

$$2(D+1) > (d+\delta)m. \tag{7.10}$$

There there exist $P, Q \in \mathbb{Z}[X]$, not both zero, with
(i) $\max\{\deg P, \deg Q\} \le D$,
(ii) $\max\{\|P\|, \|Q\|\} \le c_2(\alpha)^{D/\delta}$ *where* $c_2(\alpha) = 8^d c_1(\alpha)^{2d}$ *with* $c_1(\alpha)$ *as in Lemma 7.3.1,*
(iii) $P - \alpha Q \in \mathbb{C}[X]$ *is different from* 0 *and vanishes at* α *with multiplicity at least* m.

Proof. We set $P = \sum_{j=0}^D p_j X^j$ and $Q = \sum_{j=0}^D q_j X^j$, where p_j, q_j are unknowns for the moment.
For a fixed choice of these coefficients, $R = P - \alpha Q$ is a polynomial. The assertion (iii) is satisfied if R vanishes in α with multiplicity m, i.e., $(d^iR/dX^i)(\alpha) = 0$ for all $i \in \{0, \ldots, m-1\}$. In concrete,

$$\sum_{j=0}^{D} j(j-1)\cdots(j-i+1)(p_j\alpha^{j-i} - q_j\alpha^{j-i+1}) = 0 \quad \text{for all} \quad i \in \{0, \ldots, m-1\}.$$

We divide by $i!$ and obtain binomial coefficients. Now we use Lemma 7.3.1 to eliminate the powers of α with exponent $\ge d$. Therefore, (iii) would follow from

$$\sum_{j=0}^{D}\sum_{k=0}^{d-1} \binom{j}{i}(p_j a_{j-i,k} - q_j a_{j-i+1,k})\alpha^k = 0 \quad \text{for all} \quad i \in \{0, \ldots, m-1\}$$

and therefore from

$$\sum_{j=0}^{D} \binom{j}{i}(p_j a_{j-i,k} - q_j a_{j-i+1,k}) = 0 \quad \text{for all} \quad k \in \{0, \ldots, d-1\}, i \in \{0, \ldots, m-1\}.$$

This is a system of dm homogeneous linear equations with integer coefficients in the $2(D+1)$ unknowns $p_0, \ldots, p_D, q_0, \ldots, q_D$. By hypothesis $2(D+1) > (d+\delta)m > dm$, so there is a non-trivial solution $P, Q \in \mathbb{Z}[X]$. But we need a solution with "small" coefficients.

For this we use Siegel's Lemma. We construct a matrix $A \in \mathrm{M}_{MN}(\mathbb{Z})$, whose rows are given by our equations. We set $M = dm$ and $N = 2(D+1)$.
The entries of A are of the form $\binom{j}{i} a_{j-i,k}$ and $-\binom{j}{i} a_{j-i+1,k}$. As $\binom{j}{i} \leq 2^j \leq 2^D$, we find that

$$\|A\| \leq 2^D \max_{j \leq D+1, 0 \leq k \leq d-1} |a_{jk}| \leq 2^D c_1(\alpha)^{D+1},$$

using Lemma 7.3.1.
We set $B = 2^D c_1(\alpha)^{D+1}$. The exponent in Siegel's Lemma is

$$M/(N-M) = dm/(2(D+1) - dm) < dm/(\delta m) = d/\delta$$

by (7.10). We obtain $P, Q \in \mathbb{Z}[X]$, not both 0, of degree at most D and $\max\{\|P\|, \|Q\|\} \leq (2(D+1)B)^{d/\delta} \leq (2 \cdot 2^D 2^D c_1(\alpha)^{D+1})^{d/\delta} \leq c_2(\alpha)^{D/\delta}$ with $c_2(\alpha) = 8^d c_1(\alpha)^{2d}$. We get the bound in (ii). By construction also (i) holds.
By construction α is a root of order at least m of $P - \alpha Q$. The polynomial $P - \alpha Q$ is not identically zero since $(P, Q) \neq (0, 0)$ and $\alpha \notin \mathbb{Q}$. We then get (iii). □

7.4 Proof of Thue's Theorem

We need a multiplicity estimate first. The prototype is the following very simple consideration.

Remark 7.4.1. Let $P \in \mathbb{C}[X] \setminus \{0\}$ be a polynomial and $z \in \mathbb{C}$. We write $\mathrm{ord}_z P$ for the order of vanishing of P in z, i.e., $P = (X-z)^{\mathrm{ord}_z P} R$ with $R \in \mathbb{C}[X]$ and $R(z) \neq 0$. If $z_1, \ldots, z_E \in \mathbb{C}$ are pairwise distinct, there exists $R \in \mathbb{C}[X]$ with

$$P = (X - z_1)^{\mathrm{ord}_{z_1} P} \cdots (X - z_E)^{\mathrm{ord}_{z_E} P} R$$

and $R(z_e) \neq 0$ for all e. We compare degrees and obtain

$$\sum_{e=1}^{E} \mathrm{ord}_{z_e} P \leq \deg P.$$

This very simple estimate will not be sufficient for our purposes, because we will also need to vary P in addition to the z_e.

Lemma 7.4.2. *Let $D, d \geq 1$ be integers, $z_0, \ldots, z_d \in \mathbb{C}$ be pairwise distinct and $\theta_0, \ldots, \theta_d \in \mathbb{C}$ be arbitrary. Let $P, Q \in \mathbb{C}[X]$ be polynomials of degree at most D. If $P - \mu Q \neq 0$ for any $\mu \in \mathbb{C}$, we have*

$$\sum_{i=0}^{d} \mathrm{ord}_{z_i}(P - \theta_i Q) \leq d + 2D.$$

The lemma is trivial if all the θ_i are equal (or $d = 0$) because we are in the situation of Remark 7.4.1. In this case the bound is not optimal at all as D would suffice. For our proof we need additional flexibility.

Proof. We write w_i for the order of vanishing of $R = P - \theta_i Q$ in z_i. If $w_i \geq 1$, the derivative $R' = P' - \theta_i Q'$ has a root of order $w_i - 1$ in z_i. In this case, z_i is a root of

$$W = RQ' - R'Q = (P - \theta_i Q)Q' - (P' - \theta_i Q')Q = PQ' - P'Q.$$

of order $\geq w_i - 1$. But W does not depend on $i \in \{0, \dots, d\}$ as we have eliminated θ_i. Note that $W = 0$ implies that P and Q are proportional (look at the derivative of P/Q) and this is not possible by our hypothesis.
We write down the easy observation we made above in the following way

$$\sum_{i=0}^{d} w_i \leq \sum_{i=0}^{d} \left(1 + \operatorname{ord}_{z_i}(PQ' - P'Q)\right).$$

Since $z_0, \dots, z_d$ are pairwise distinct, the right-hand side is at most

$$(d+1) + \deg(PQ' - P'Q) \leq (d+1) + 2D - 1 = d + 2D.$$

The lemma follows. □

We now start with the proof of Thue's Theorem. We assume that $\alpha \in \mathbb{C}$ is algebraic of degree $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. We fix $\epsilon > 0$. We start with an easy reduction.

(i) In case $\alpha \in \mathbb{Q}$, we have seen a better bound in Remark 7.1.7. We are then going to assume $d \geq 2$, i.e., that α is irrational.

(ii) We know that there is a rational integer $N \geq 1$ such that $N\alpha$ is an algebraic integer. Since $[\mathbb{Q}(N\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = d$, we are allowed to replace α by $N\alpha$. Therefore, we may and are going to assume that α is an algebraic integer.

(iii) Finally, we are allowed to assume that there is a very good approximation to α. Concretely, there are integers $a, b \in \mathbb{Z}$ with $b \geq 1$ and such that

$$\left|\alpha - \frac{a}{b}\right| \leq \frac{1}{b^{1+d/2+\epsilon}}.$$

Otherwise the theorem would be trivially true. In particular, we have $|\alpha - a/b| \leq 1$. Moreover, we may assume that b is sufficiently large depending on α, otherwise we would have finitely many possible choices for (a, b) and this would give the claim.

Remark 7.4.3. Here is an overview of the strategy.

(i) Using Proposition 7.3.2 we construct the polynomials $P, Q \in \mathbb{Z}[X]$ with the three properties. For this we must give parameters D, δ, m so that (7.10) is satisfied. We are going to choose these parameters later.
In particular, $P - \alpha Q$ vanishes at α with multiplicity at least m and we have $\deg P, \deg Q \leq D$.

(ii) As $P - \alpha Q$ takes "small" values close to α and since α is well approximated by a/b, the number $P(a/b) - \alpha Q(a/b)$ is small and thus $P(a/b)/Q(a/b)$ approximates α. The quality of the approximation can be controlled using the parameters D, δ, m. The auxiliary polynomial has the effect of enhancing the quality of the approximation.

Now, $x_0 = b^D P(a/b)$ and $y_0 = b^D Q(a/b)$ are integers. If $y_0 \neq 0$, then x_0/y_0 is very close to α.
If x/y is an approximation of α with $x, y \in \mathbb{Z}$ and $y \geq 1$, we have the trivial inequality

$$\left| y_0 \left(\alpha - \frac{x}{y} \right) \right| = \left| y_0 \left(\alpha - \frac{x}{y} \right) - x_0 + x_0 \right| \geq \left| x_0 - y_0 \frac{x}{y} \right| - |y_0 \alpha - x_0|.$$

If $x_0/y_0 \neq x/y$, we also have $|x_0 - y_0 x/y| = |(x_0 y - y_0 x)/y| \geq 1/y$. Thus

$$\left| y_0 \left(\alpha - \frac{x}{y} \right) \right| \geq \frac{1}{y} - |y_0 \alpha - x_0|.$$

With a suitable choice of parameters we will get $|y_0\alpha - x_0|$ smaller than $1/(2y)$ and with that we get a non-trivial bound on the right hand side. The final claim will then follow after cleverly choosing the parameters.

(iii) What happens if $x_0/y_0 = x/y$? We recall that x_0, y_0 are constructed using the auxiliary polynomials P and Q. But P and Q come Siegel's Lemma and we have little control on these polynomials.
In this case we have $P(a/b) - \frac{x}{y} Q(a/b) = 0$. In other words, a/b is a root of $P - \frac{x}{y} Q$. With the help of Lemma 7.4.2 we are going to be able to show that the order of vanishing of $P - \frac{x}{y} Q$ in a/b is not "too large". This means that, instead of P and Q we have to work with derivatives.
In the context of Thue's theorem, this step is a problem that we can solve with a little algebra, i.e. Lemma 7.4.2.
To prove Roth's theorem one has to work with auxiliary polynomials that have > 2 variables. This step represents the main difficulty for Roth's theorem.

Now let's put that strategy into action and fill in the details.

Remark 7.4.4. We have just introduced in Proposition 7.3.2 the quantity $c_2(\alpha) > 0$. It depends only on α. Later we are going to tacitly introduce further constants $c_3(\alpha), c_4(\alpha), \ldots$. These will depend only on α and not on a, b nor x, y nor the choice of parameters D, m, δ nor the quantity n.

In order to anticipate the problem described in (iii) above we define two sequences of integers x_n, y_n using the derivatives of P and Q.
Let us suppose for the moment that we have fixed the parameters $D, m \in \mathbb{Z}^{>0}$ and $\delta \in (0, 1/2]$ and are given the polynomials P and Q as in Proposition 7.3.2.
Let $n \geq 0$ be an integer. Write $Q = \sum_{j=0}^{D} q_j X^j$. We have $\frac{1}{n!} d^n Q / dX^n = \sum_{j=0}^{D} q_j \binom{j}{n} X^{j-n} \in \mathbb{Z}[X]$. Substituting a/b and multiplying by b^D we obtain the equality

$$\frac{b^D}{n!} \frac{d^n Q}{dX^n} \left(\frac{a}{b} \right) = \sum_{j=0}^{D} q_j \binom{j}{n} \left(\frac{a}{b} \right)^{j-n} b^D \in \mathbb{Z}.$$

For every integer $n \geq 0$ we define

$$x_n = \frac{b^D}{(n)!} \frac{d^n P}{dX^n} \left(\frac{a}{b} \right) \quad \text{and} \quad y_n = \frac{b^D}{(n)!} \frac{d^n Q}{dX^n} \left(\frac{a}{b} \right). \tag{7.11}$$

Lemma 7.4.5. *For every integer $n \geq 0$, the numbers x_n, y_n are integers and $|y_n| \leq c_3(\alpha)^{D/\delta} b^D$.*

Proof. We have just seen above that $y_n \in \mathbb{Z}$ and the same clearly holds for $x_n \in \mathbb{Z}$.
We have $|y_n| \leq b^D \sum_{j=0}^{D} |q_j \binom{j}{n} (a/b)^{j-n}|$. We are going to use the bound for $|q_j|$ from Proposition 7.3.2. We have $|q_j| \leq c_2(\alpha)^{D/\delta}$ for all j. Moreover we have $|a/b - \alpha| \leq 1$ and therefore $|a/b| \leq 1 + |\alpha|$. It follows that

$$|y_n| \leq b^D c_2(\alpha)^{D/\delta} (1 + |\alpha|)^D \sum_{j=0}^{D} \binom{j}{n} \leq b^D c_2(\alpha)^{D/\delta} (1 + |\alpha|)^D 2^{D+1}.$$

The last inequality follows by $\binom{j}{n} \leq 2^j$ and $\sum_{j=0}^{D} 2^j = 2^{D+1} - 1$.
We are done by setting $c_3(\alpha) = 4c_2(\alpha)(1 + |\alpha|)$ (recall that $\delta \leq 1/2$). □

Next we want to verify that $|y_n\alpha - x_n|$ is small for all $n \in \{0, \ldots, m\}$. In case $y_n \neq 0$ this implies that x_n/y_n is close to α.

Lemma 7.4.6. *For all $n \in \{0, \ldots, m\}$ we have $|x_n - y_n\alpha| \leq c_4(\alpha)^{D/\delta} b^D \left|\alpha - \frac{a}{b}\right|^{m-n}$.*

Note that the better the approximation a/b of α is, the smaller $y_n\alpha - x_n$ is going to be.

Proof. We write $R = P - \alpha Q \in \mathbb{Z}[\alpha][X]$. Then

$$\frac{d^k R}{dX^k}(\alpha) = 0$$

for all $k \in \{0, \ldots, m-1\}$, as, by the construction in Proposition 7.3.2, our auxiliary polynomial vanishes in α with multiplicity $\geq m$.
The Taylor expansion of R around α is

$$R = \sum_{k=m}^{D} \frac{1}{k!} \frac{d^k R}{dX^k}(\alpha)(X - \alpha)^k.$$

Only the derivatives up to the order D have to be taken into account. Let $n \geq 0$ be an integer. We derive this equality n times, multiply by $b^D/n!$ and find

$$\frac{b^D}{n!} \frac{d^n R}{dX^n} = b^D \sum_{k=m}^{D} \frac{1}{k!} \frac{d^k R}{dX^k}(\alpha) \binom{k}{n} (X - \alpha)^{k-n},$$

We substitute a/b and obtain

$$x_n - \alpha y_n = b^D \sum_{k=m}^{D} \binom{k}{n} \frac{1}{k!} \frac{d^k R}{dX^k}(\alpha) \left(\frac{a}{b} - \alpha\right)^{k-n} \tag{7.12}$$

by (7.11).

Proposition 7.3.2 gives a bound on the coefficients of P and Q. To be more precise, if $P = \sum_{j=0}^{D} p_j X^j$ and $Q = \sum_{j=0}^{D} q_j X^j$ we have $\max_j\{|p_j|, |q_j|\} \leq c_2(\alpha)^{D/\delta}$. Now, $\frac{1}{k!} d^k R/dX^k = \sum_{j=0}^{D} \binom{j}{k}(p_j - \alpha q_j) X^{j-k}$. This, together with the triangle inequality, gives

$$\left|\frac{1}{k!}\frac{d^k R}{dX^k}(\alpha)\right| \leq \sum_{j=0}^{D} \binom{j}{k}(|p_j| + |\alpha||q_j|)|\alpha|^{j-k} \leq 2c_2(\alpha)^{D/\delta} \max\{1, |\alpha|\}^{D+1} 2^{D+1}.$$

We now use this in (7.12) and recall that $|\alpha - a/b| \leq 1$. We have

$$\begin{aligned} |x_n - \alpha y_n| &\leq b^D \left|\alpha - \frac{a}{b}\right|^{m-n} 2c_2(\alpha)^{D/\delta} \max\{1, |\alpha|\}^{D+1} 2^{D+1} \sum_{k=m}^{D} \binom{k}{n} \\ &\leq b^D \left|\alpha - \frac{a}{b}\right|^{m-n} c_2(\alpha)^{D/\delta} \max\{1, |\alpha|\}^{D+1} 2^{2D+3}. \end{aligned}$$

Since $\delta \leq 1$ we obtain $|x_n - \alpha y_n| \leq c_4(\alpha)^{D/\delta} b^D |\alpha - a/b|^{m-n}$, where we set $c_4(\alpha) = 32 \max\{1, |\alpha|\}^2 c_2(\alpha)$. This gives our lemma. □

Roughly speaking, x_n/y_n is a good approximation of α. But we have to be a little careful. First of all it is not clear that $y_n \neq 0$. Second, even if $y_n \neq 0$, we do not know a priori that x_n/y_n is actually a new approximation. This will be the case for some not too large n. We are able to show this with the help of Lemma 7.4.2.
But first we must choose the parameter D as a function of d, δ and m as follows

$$D = \left\lfloor \frac{(d + 2\delta)m}{2} \right\rfloor. \tag{7.13}$$

We have then $D + 1 > (d + 2\delta)m/2 = dm/2 + \delta m$ and thus $2(D + 1) > (d + 2\delta)m$. This choice of D satisfies the hypothesis (7.10). As $dm \geq 2$ we also have that $D \geq 1$.

Lemma 7.4.7. *Let $\theta \in \mathbb{C}$. There exists an integer $n \geq 0$ with $n \leq 2\delta m + d$ and $x_n - \theta y_n \neq 0$.*

Proof. We consider two cases:
Case 1. There exists μ with $P - \mu Q = 0$. The auxiliary function $R = P - \alpha Q$ becomes $R = (\mu - \alpha)Q$. By Proposition 7.3.2, R vanishes in α with multiplicity $\geq m$ and $R \neq 0$. But R is a multiple of Q which has rational coefficients. Therefore, R and all its derivatives up to order $m - 1$ must vanish at all $\sigma(\alpha)$, for all embeddings $\sigma : \mathbb{Q}(\alpha) \to \mathbb{C}$. The number of distinct $\sigma(\alpha)$ is exactly $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ and thus R has at least dm roots counted with multiplicities. It follows that $\deg R \geq dm$ which is the trivial bound in Remark 7.4.1. On the other hand we have $\deg R = \deg Q \leq D$ by construction. Then, $dm \leq D$. The choice (7.13) implies that $D \leq (d + 2\delta)m/2$. Combining these two bounds for D we see that $2dm \leq dm + 2\delta m$, therefore $2m \leq dm \leq 2m\delta < 2m$ a contradiction. Case 1 is then impossible.
Case 2. We have $P - \mu Q \neq 0$ for every $\mu \in \mathbb{C}$. We must show that $\mathrm{ord}_{a/b}(P - \theta Q) \leq 2\delta m + d$.

By construction the polynomial $P - \alpha Q \neq 0$ vanishes in α with order $\geq m$. As in the first case, $P - \sigma(\alpha)Q$ must vanish in $\sigma(\alpha)$ with the same order $\geq m$, for all d embeddings $\sigma\colon \mathbb{Q}(\alpha) \to \mathbb{C}$.
We apply Lemma 7.4.2 to $z_0 = a/b$ and $\{z_1, \ldots, z_d\} = \{\sigma(\alpha) : \sigma\colon \mathbb{Q}(\alpha) \to \mathbb{C}\}$ with $\theta_0 = \theta$ and $\theta_i = z_i$ for all $i \in \{1, \ldots, d\}$. The Lemma implies

$$\operatorname{ord}_{a/b}(P - \theta Q) + md \leq \sum_{i=0}^{d} \operatorname{ord}_{z_i}(P - \theta_i Q) \leq 2D + d.$$

Then, by, (7.13)

$$\operatorname{ord}_{a/b}(P - \theta Q) \leq 2D + d - md \leq 2\delta m + d,$$

and we are finished with the second case. □

We now come to a key estimate.

Theorem 7.4.8. *Let α be an algebraic integer with $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d \geq 2$ and let $\epsilon > 0$. There exists a constant $T = T(\alpha, \epsilon) > 1$ with the following property. If there exist $a, b \in \mathbb{Z}$ with $b > T$ and*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{1+d/2+\epsilon}}, \tag{7.14}$$

then we have

$$\left|\alpha - \frac{x}{y}\right| \geq \frac{C(\alpha, \epsilon)}{y^{1+d/2+2\epsilon}}$$

for all $x, y \in \mathbb{Z}$ with $y \geq 1$. Here $C(\alpha, \epsilon) > 0$ depends only on α and ϵ.

Proof. Fix $x, y \in \mathbb{Z}$ with $y \geq 1$.
We keep the notation with our parameters D, m, and $\delta \in (0, 1/4]$. We have already chosen D in (7.13). We are going to choose δ as a function of ϵ and d and m as a function of α, ϵ, y, b. For the moment we just set the condition

$$m \geq \frac{d}{\delta} \tag{7.15}$$

on m.
We fix a real $T > 1$. Later we are going to take it large enough in terms of ϵ, d, δ and the constants $c_3(\alpha), c_4(\alpha)$ given by Lemmas 7.4.5 and 7.4.6.
We assume that we have a and b as in the hypothesis.
Proposition 7.3.2 gives polynomials P and Q and we construct x_n, y_n as in (7.11).
We let m be free and choose n as in Lemma 7.4.7 applied to $\theta = x/y$, so $n \geq 0$, $n \leq 2\delta m + d$ and $x_n - y_n \frac{x}{y} \neq 0$. Because $m \geq d/\delta$ and $\delta < 1/3$ we have that

$$m - n \geq m - 2\delta m - d \geq m - 3\delta m = m(1 - 3\delta) > 0. \tag{7.16}$$

In particular $n < m$ and we may apply Lemma 7.4.6.

We have the trivial inequality

$$\left|x_n - y_n\frac{x}{y}\right| \leq |x_n - \alpha y_n| + \left|y_n\left(\frac{x}{y} - \alpha\right)\right|.$$

The critical observation is that, since the expression on the left is non-zero, it is a positive rational number with denominator which is a divisor of y. Therefore, we have $|x_n - y_n\frac{x}{y}| \geq 1/y$.
We write down the fundamental inequality

$$\frac{1}{y} \leq |x_n - \alpha y_n| + \left|y_n\left(\frac{x}{y} - \alpha\right)\right|. \tag{7.17}$$

for later.
We will now estimate $|x_n - \alpha y_n|$ from above. By Lemma 7.4.6 we have

$$\begin{aligned}|x_n - \alpha y_n| &\leq c_4(\alpha)^{D/\delta} b^D \left|\alpha - \frac{a}{b}\right|^{m-n} \\ &\leq c_4(\alpha)^{D/\delta} b^D \frac{1}{b^{(1+d/2+\epsilon)(m-n)}} \\ &\leq c_4(\alpha)^{D/\delta} b^D \frac{1}{b^{(1+d/2+\epsilon)m(1-3\delta)}}\end{aligned}$$

where we have used (7.14) and (7.16).
We can estimate the exponents D and D/δ using the choice (7.13) and see that $D \leq dm/2 + 2\delta m \leq dm$. Therefore,

$$|x_n - \alpha y_n| \leq c_4(\alpha)^{dm/\delta} \frac{b^{dm/2+2\delta m}}{b^{(1+d/2+\epsilon)m(1-3\delta)}} = c_4(\alpha)^{dm/\delta} \frac{1}{b^{((1+d/2+\epsilon)(1-3\delta)-d/2-2\delta)m}}.$$

For $\delta = 0$ the exponent of b^m is equal to $1+\epsilon$. Therefore, if we choose (and we do that) δ small enough as a function of ϵ and d we have that the exponent of b^m is at least $1 + \epsilon/2$. We get

$$|x_n - \alpha y_n| \leq c_4(\alpha)^{dm/\delta} \frac{1}{b^{m(1+\epsilon/2)}} \leq \frac{c_4(\alpha)^{dm/\delta}}{b^m T^{m\epsilon/2}} = \frac{1}{b^m}\left(\frac{c_4(\alpha)^{d/\delta}}{T^{\epsilon/2}}\right)^m,$$

as $b > T$. But we may take T large enough so that $c_4(\alpha)^{d/\delta}/T^{\epsilon/2} < 1$, thus

$$|x_n - \alpha y_n| \leq \frac{1}{b^m}. \tag{7.18}$$

Now, the larger m the better approximation we have.
It is now time to choose m. Until now we had a lot of freedom as we only had to satisfy the condition (7.15). We now set

$$m = \left\lfloor \frac{\log(2y)}{\log b} + \frac{d}{\delta} \right\rfloor + 1 \tag{7.19}$$

so that $m \geq 1$, (7.15) holds and the right side of (7.18) is at most $1/(2y)$ and this will give something in (7.17).
By $m \geq \log(2y)/\log b$ it follows $b^{-m} \leq 1/(2y)$. This gives

$$|x_n - \alpha y_n| \leq \frac{1}{2y}.$$

By (7.17), we have

$$\frac{1}{2y} \leq |y_n| \left|\alpha - \frac{x}{y}\right|.$$

The absolute value $|y_n|$ can be bounded with the help of Lemma 7.4.5. It follows that

$$\frac{1}{2y} \leq c_3(\alpha)^{D/\delta} b^D \left|\alpha - \frac{x}{y}\right|.$$

Earlier we have seen that $D \leq dm/2 + 2\delta m$ and $D/\delta \leq dm/\delta$. It follows that

$$\frac{1}{2y} \leq c_3(\alpha)^{dm/\delta} b^{(d/2+\delta)m} \left|\alpha - \frac{x}{y}\right|. \tag{7.20}$$

The choice (7.19) implies that $m \leq \frac{\log(2y)}{\log b} + \frac{d}{\delta} + 1 \leq \frac{\log(2y)}{\log T} + \frac{d}{\delta} + 1$. Therefore

$$c_3(\alpha)^{dm/\delta} \leq c_3(\alpha)^{\frac{d\log(2y)}{\delta \log T}} c_3(\alpha)^{(d/\delta)^2 + d/\delta} = c_3(\alpha)^{(d/\delta)^2+d/\delta} (2y)^{\frac{d \log c_3(\alpha)}{\delta \log T}},$$

and

$$b^{(d/2+\delta)m} \leq b^{(d/2+\delta)(d/\delta+1)} b^{(d/2+\delta)(\log(2y))/\log b} = b^{(d/2+\delta)(d/\delta+1)} (2y)^{d/2+\delta}.$$

We may take T large enough depending on α and δ, so we may assume $c_3(\alpha)^{dm/\delta} \leq c_3(\alpha)^{(d/\delta)^2+d/\delta}(2y)^{\epsilon}$. We use these two upper bounds in (7.20) and find

$$\frac{1}{2y^{1+d/2+\delta+\epsilon}} \leq c_3(\alpha)^{(d/\delta)^2+d/\delta} b^{(d/2+\delta)(d/\delta+1)} 2^{\epsilon} 2^{d/2+\delta} \left|\alpha - \frac{x}{y}\right|.$$

Except for δ, all parameters have disappeared. We may assume $\delta \leq \epsilon$ and then replace δ by ϵ.
We are finally done with the proof of the theorem. □

Thue's Theorem is now a simple consequence.

Proof of Thue's Theorem 7.1.6. Without loss of generality we may assume that α is an irrational algebraic integer. Let T be as in Theorem 7.4.8. There are two cases:
We consider the inequality

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{y^{1+d/2+\epsilon/2}} \tag{7.21}$$

with $x, y \in \mathbb{Z}$ and $y \geq 1$.

Case 1. Suppose $y \leq T$ for all $x, y \in \mathbb{Z}$, which satisfy this inequality. Then we are considering at most finitely many y. As $|x - \alpha y| < 1$ we have only two possible values of x for every y. It then follows

$$\left|\alpha - \frac{x}{y}\right| \geq \frac{C(\alpha, \epsilon)}{y^{1+d/2+\epsilon/2}} \geq \frac{C(\alpha, \epsilon)}{y^{1+d/2+\epsilon}}$$

for all $x, y \in \mathbb{Z}$, where $C(\alpha, \epsilon) > 0$ only depends on α and ϵ.
Case 2. Suppose there are $x, y \in \mathbb{Z}$ with $y > T$ which satisfy the inequality. The claim follows by Theorem 7.4.8 with the starting values $a = x$ and $b = y$ and with $\epsilon/2$. □

Remark 7.4.9. We conclude with a remark on effectivity. The constants $c_1(\alpha), \ldots, c_4(\alpha)$ that appear in the preparation of the proof can in principle be determined explicitly, if one knows the minimal polynomial of α over $\mathbb{Q}$. However, the final constant $C(\alpha, \epsilon)$ cannot be calculated with this method.
In order to get the machinery in Theorem 7.4.8 to start, one needs a "starting approximation" a/b.
Case 1. There exists no starting approximation with $b > T$ and satisfying (7.14). Then the Theorem is trivially true and one must simply consider the finitely many $(x, y) \in \mathbb{Z}^2$ mit $1 \leq y \leq T$ and $|x - y\alpha| < 1$, and find a constant $C(\alpha, \epsilon)$ that works.
Case 2. There exists a start approximation a/b with $b > T$ and satisfying (7.14). Theorem 7.4.8 gives a constant that depends on a and b.
In general it is not possible to decide in which case we fall.
Since the value of T is already very large for "simple" α, it is rather unlikely that one is in case 2. But that cannot be ruled out in practice.

8 The abc-Conjecture

8.1 The conjecture and some consequences

The *abc*-conjecture was formulated in different versions in the 1980s. Its importance is due on the one hand to the fact that it is very easy to formulate, on the other hand to the many deep consequences it has. The conjecture is still open.
We are going to see a formulation due to Joseph Oesterlé and David Masser. The related Szpiro Conjecture one elliptic curves appeared a bit earlier.

Definition 8.1.1. Let $n \in \mathbb{Z} \setminus \{0\}$ The **radical** $\mathrm{rad}(n)$ of n is the product

$$\prod_{p|n} p$$

of the prime numbers p that divide n.

Conjecture (*abc*-Conjecture, Masser and Oesterlé)**.** *For all $\epsilon > 0$ there exists a constant $K(\epsilon) > 0$ with the following property. For all coprime $a, b, c \in \mathbb{N}$ with $a + b = c$ we have*

$$c \leq K(\epsilon)\mathrm{rad}(abc)^{1+\epsilon}.$$

Remark 8.1.2. It is easy to see that the conjecture is equivalent to a version with the apparently stronger conclusion:

$$\max\{|a|, |b|, |c|\} \leq K(\epsilon)\mathrm{rad}(abc)^{1+\epsilon}$$

for all coprime $a, b, c \in \mathbb{Z} \setminus \{0\}$ with $a + b = c$.

A well-known consequence of *abc* is an asymptotic version of Fermat's Last Theorem

Lemma 8.1.3. *Assume that the abc-Conjecture holds. There exists a constant C with the following property. Let $x, y, z, n \in \mathbb{Z}^{>0}$ with x, y, z coprime, $x^n + y^n = z^n$ and $n \geq 4$, We have* $\max\{x, y, z, n\} \leq C$.

Proof. We use the conjecture with $a = x^n, b = y^n, c = z^n$ and $\epsilon = 1/4$. By hypothesis, a, b, c are coprime. We have $z^n \leq K\mathrm{rad}(abc)^{5/4}$. We note that $\mathrm{rad}(abc) = \mathrm{rad}(xyz) \leq xyz$.
Since $x \leq z$ and $y \leq z$ we have $z^n \leq K \cdot (xyz)^{5/4} \leq K \cdot z^{15/4}$. But $n \geq 4$ and then $z^{1/4} = z^{4-15/4} \leq K$. It follows that $\max\{x, y, z\} = z \leq K^4$. Now, $z \geq 2$ since $x \geq 1$ and $y \geq 1$. Therefore, $2^{n-15/4} \leq z^{n-15/4} \leq K$ and also n is bounded by a function of K. □

Remark 8.1.4. We now see that in the statement of the *abc*-Conjecture one cannot choose $\epsilon = 0$.
Let $p \geq 3$ be a prime number and

$$a = 1, \quad b = 2^{p(p-1)} - 1, \quad c = a + b = 2^{p(p-1)}.$$

Clearly these three numbers are coprime. Since 2 and p are coprime we have $2^{p(p-1)} \equiv 1 \pmod{p^2}$, by Euler's Theorem. Therefore, $p^2 \mid b$ that implies $\mathrm{rad}(b) \leq b/p$. We conclude that $\mathrm{rad}(abc) = \mathrm{rad}(bc) = 2\mathrm{rad}(b) \leq 2b/p$.
Finally, the fraction

$$\frac{c}{\mathrm{rad}(abc)} = \frac{b+1}{\mathrm{rad}(abc)} \geq p\frac{b+1}{2b} \geq \frac{p}{2}$$

in unbounded since we may take p as large as we want.

Even the fact that c can be bounded as a function of $\mathrm{rad}(abc)$ is not obvious. The following result by Stewart and Yu gives an exponential bound.

Theorem 8.1.5 (Stewart-Yu 2001)**.** *For all $\epsilon > 0$ there is a constant $K(\epsilon) > 0$ with the following property. For coprime $a, b, c \in \mathbb{N}$ with $a + b = c$ we have*

$$c \leq e^{K(\epsilon)\mathrm{rad}(abc)^{1/3+\epsilon}}.$$

Note that this bound is not enough to prove Lemma 8.1.3.
We are going to see another application of the conjecture. The following theorem is a generalization of Thue's Theorem which we proved in Chapter 7.

Theorem 8.1.6 (Roth 1955)**.** *Let $\alpha \in \mathbb{C}$ be an algebraic number. For all $\epsilon > 0$ there is a constant $C(\alpha, \epsilon) > 0$ such that*

$$\left|\alpha - \frac{x}{y}\right| \geq \frac{C(\alpha, \epsilon)}{y^{2+\epsilon}}$$

for all $x, y \in \mathbb{Z}$ with $y \geq 1$ and $x/y \neq \alpha$.

We are going to prove the following at the end of this chapter.

Theorem 8.1.7. *The abc-Conjecture implies Roth's Theorem.*

8.2 The Theorem of Mason–Stothers

The Theorem of Mason and Stothers can serve as motivation for the *abc*-Conjecture. We need to introduce the radical of a polynomial.

Definition 8.2.1. Let K be an algebraically closed field and $P = p_0 \prod_{i=1}^{g} (X - \lambda_i)^{e_i} \in K[X] \setminus \{0\}$ with $\lambda_1, \ldots, \lambda_g \in K$ pairwise distinct and $e_1, \ldots, e_g \in \mathbb{Z}^{>0}$. The **radical** of P is

$$\mathrm{rad}(P) = \prod_{i=1}^{g} (X - \lambda_i) \in K[X].$$

Example 8.2.2. For $P = (X-1)^2$ we have $\mathrm{rad}(P) = X - 1$. If P is a monic polynomial without multiple roots then clearly $\mathrm{rad}(P) = P$. In general $\deg \mathrm{rad} P$ is the number of roots of P in K.

Theorem 8.2.3 (Mason–Stother)**.** *Let K be an algebraically closed fields of characteristic 0. Let $A, B, C \in K[X] \setminus \{0\}$ be coprime and not all constant with $A + B = C$. Then,*

$$\max\{\deg A, \deg B, \deg C\} \leq \deg \mathrm{rad}(ABC) - 1.$$

Let us compare this Theorem with the *abc*-Conjecture. The polynomials A, B, C play the roles of the positive integers a, b, c. Moreover, $\deg A$ plays the role of $\log a$ and $\deg \mathrm{rad}(ABC)$ the role of $\log \mathrm{rad}(abc)$. In particular, for polynomials it is possible to take $\epsilon = 0$ in contrast to what happens for natural numbers.

Remark 8.2.4. Without any further restriction, the above theorem does not hold in positive characteristic. Let K be a field of characteristic $p > 0$. Then we have $(X-1)^p + 1 = X^p$ in $K[X]$. We set $A = (X-1)^p, B = 1$ and $C = X^p$. Then, $\max\{\deg A, \deg B, \deg C\} = p$, but $\deg \mathrm{rad}(ABC) = \deg \mathrm{rad}(X(X-1)) = 2$.

The proof of Theorem 8.2.3 is elementary and we are going to give a proof here using the Riemann–Hurwitz formula for the projective line.
Let K be an algebraically closed field of characteristic 0 and $P, Q \in K[X]$ coprime with $Q \neq 0$. We consider the quotient $f = P/Q$ as rational function $\mathbb{P}^1(K) \to \mathbb{P}^1(K)$ as in Section 5.2. As we have done before we see the set $\mathbb{P}^1(K)$ as $K \cup \{\infty\}$, by identifying $x \in K$ with $[1 : x] \in \mathbb{P}^1(K)$ and ∞ is the point $[0 : 1]$.

Definition 8.2.5. Let $x \in \mathbb{P}^1(K)$. For $x \in K$ we denote by $\mathrm{ord}_x(P)$ the order of vanishing P at x and $\mathrm{ord}_\infty(P) = -\deg P$. We define moreover $\mathrm{ord}_x(f) = \mathrm{ord}_x(P) - \mathrm{ord}_x(Q)$. If $f \notin K$, the **ramification index** $e_x(f)$ of f at $x \in \mathbb{P}^1(K)$ is equal to

$$e_x(f) = \begin{cases} \mathrm{ord}_x(f - f(x)) & : \text{if } f(x) \neq \infty, \\ \mathrm{ord}_x(f^{-1}) & : \text{if } f(x) = \infty. \end{cases}$$

If $e_x(f) = 1$, we say that f is **unramified** at the point x. If f is not unramified at x we say it is **ramified** at x. The value $f(x)$ at some ramified point x is called **branch point** of f.

Since the couple (P, Q) is determined up to a non-zero constant, the ramification index $e_x(f)$ is well defined. We moreover have $e_x(f) \in \{1, 2, \ldots\}$.

Example 8.2.6. Let $K = \mathbb{C}$. The rational function $f = X^2 + 1$ is unramified at $x = 1$, since $X^2 + 1 - f(1) = X^2 - 1$ only has simple roots. It is ramified at $x = 0$ because $X^2 + 1 - f(0) = X^2$ has a double root.

Remark 8.2.7. Let $f = P/Q$ as in Definition 8.2.5. We recall that K is an algebraically closed field of characteristic 0. If $x \in K$ with $f(x) \neq \infty$, then

$$\mathrm{ord}_x(f - f(x)) = \mathrm{ord}_x\left(\frac{P}{Q}\right)' + 1 = \mathrm{ord}_x\left(\frac{P'Q - PQ'}{Q^2}\right) + 1.$$

Recall that P and Q are coprime and $Q \neq 0$. If $P \neq 0$ we have defined $\deg f = \max\{\deg P, \deg Q\}$ for $f = P/Q$.

Theorem 8.2.8 (Riemann–Hurwitz for $\mathbb{P}^1$)**.** *Let K, P, Q with K of characteristic 0 and $f = P/Q \notin K$ as above. There are at most finitely many $x \in \mathbb{P}^1(K)$, such that $e_x(f) \geq 2$ and*

$$\sum_{x \in \mathbb{P}^1(K)} (e_x(f) - 1) = 2 \deg f - 2.$$

Proof. If $e_x(f) \geq 2$ for an $x \in K$ with $f(x) \neq \infty$, then $f - f(x)$ has a multiple root x. This means that $P'Q - PQ'$ vanishes at x. But $P'Q \neq PQ'$ since P, Q are coprime and f is not constant. Therefore x lies in the finite set of roots of $P'Q - PQ'$. The first claim follows from this and from the fact that $f^{-1}(\{\infty\})$ is a subset of $\{z \in K : Q(z) = 0\} \cup \{\infty\}$ which is finite.
We now consider the value of $e_x(f) - 1$ in two cases.
For $x \neq \infty$ and $Q(x) \neq 0$, we have $e_x(f) - 1 = \operatorname{ord}_x(P/Q - f(x)) - 1 = \operatorname{ord}_x(P'Q - PQ')$ by the remark above.
If $x \neq \infty$ and $Q(x) = 0$, then $P(x) \neq 0$ and, by definition, $e_x(f) - 1 = \operatorname{ord}_x(Q) - 1$. But we note that $\operatorname{ord}_x(Q) - 1 = \operatorname{ord}_x(Q') = \operatorname{ord}_x(P'Q - PQ')$, as above.
We set $S = \sum_{x \in \mathbb{P}^1(K)} (e_x(f) - 1)$. We have

$$\begin{aligned} S = e_\infty(f) - 1 + \sum_{x \in K} (e_x(f) - 1) &= e_\infty(f) - 1 + \sum_{x \in K} \operatorname{ord}_x(P'Q - PQ') \\ &= e_\infty(f) - 1 + \deg(P'Q - PQ'). \end{aligned}$$

Finally we must estimate $e_\infty(f)$. We consider three cases. In the first two we make use of the fact that, if P and Q have different degrees, then $\deg(P'Q - PQ') = \deg P' + \deg Q = \deg P + \deg Q'$, since the leading terms of $P'Q$ and PQ' cannot cancel each other.
First assume $\deg P > \deg Q$, so $f(\infty) = \infty$ and $e_\infty(f) = \deg P - \deg Q$. In this case we have $d = \deg f = \deg P$ and therefore $S = \deg P - \deg Q - 1 + \deg(P'Q - PQ') = \deg P - \deg Q - 1 + \deg P' + \deg Q = 2d - 2$.
Otherwise suppose $\deg P < \deg Q$ so $d = \deg Q$ and $e_\infty(f) = \operatorname{ord}_\infty(f) = \deg Q - \deg P$. Analogously as above we have $S = 2d - 2$.
Let us deal with the last case $d = \deg P = \deg Q$. Here we have $\lambda = f(\infty) \in K$ and $e_\infty(f) = \operatorname{ord}_\infty(P/Q - \lambda) = \deg Q - \deg R \geq 1$ where $R = P - Q\lambda$. Thus, $S = \deg Q - \deg R - 1 + \deg(P'Q - PQ')$. We have $P'Q - PQ' = (R' + \lambda Q')Q - (R + \lambda Q)Q' = R'Q - RQ'$. Since $\deg R \leq \deg Q - 1$ as done above we obtain $\deg(R'Q - RQ') = \deg R + \deg Q - 1$. Finally, we have $S = \deg Q - \deg R - 1 + \deg R + \deg Q - 1 = 2 \deg Q - 2 = 2d - 2$, and we are done. □

Proof of Theorem 8.2.3. We have the equality $A + B = C$. It is not possible that only one polynomial has maximal degree, therefore, possibly after permutation, we have that $\deg A = \deg B \geq \deg C$ and therefore $A, B \notin K$. We let $f = A/C \in K(X)$, so $f \notin K$ since A, C are coprime and not both constant. Moreover, $\deg f = \max\{\deg A, \deg C\} = \deg A$.

By the Riemann–Hurwitz formula for $\mathbb{P}^1$ we have

$$2\deg f - 2 = \sum_{x\in\mathbb{P}^1(K)} (e_x(f) - 1).$$

We decompose this sum in $S_0 + S_1 + S_\infty + S$ with

$$S_0 = \sum_{\substack{x\in\mathbb{P}^1(K)\\ f(x)=0}} (e_x(f)-1), \quad S_1 = \sum_{\substack{x\in\mathbb{P}^1(K)\\ f(x)=1}} (e_x(f)-1), \quad S_\infty = \sum_{\substack{x\in\mathbb{P}^1(K)\\ f(x)=\infty}} (e_x(f)-1)$$

and

$$S = \sum_{\substack{x\in\mathbb{P}^1(K)\\ f(x)\neq 0,1,\infty}} (e_x(f)-1).$$

We have

$$2\deg A - 2 = S_0 + S_1 + S_\infty + S. \tag{8.1}$$

Let $g = B/C$. Then,

$$f + g = 1 \tag{8.2}$$

and $f(\infty), g(\infty) \in K^\times \cup \{\infty\}$ (since $\deg A = \deg B \geq \deg C$).
We deal with each summand separately.
The sum S_1. Let $f(x) = 1$, then $g(x) = 0$. It follows that $x \in K$, $B(x) = 0$ and $C(x) \neq 0$. Conversely, every root $x \in K$ of B satisfies $f(x) = 1$. By definition, in this case we have $e_x(f) = \mathrm{ord}_x(A/C - 1) = \mathrm{ord}_x(g) = \mathrm{ord}_x(B)$ and thus

$$S_1 = \sum_{x\in K: B(x)=0} (\mathrm{ord}_x(B) - 1) = \deg B - \deg \mathrm{rad} B. \tag{8.3}$$

The sum S_0. Let $f(x) = 0$. Reasoing as above with A in place of B, we obtain

$$S_0 = \sum_{x\in K: A(x)=0} (\mathrm{ord}_x(A) - 1) = \deg A - \deg \mathrm{rad} A. \tag{8.4}$$

The sum S_∞. Let $f(x) = \infty$. We have $e_x(f) = \mathrm{ord}_x(f^{-1}) = \mathrm{ord}_x C - \mathrm{ord}_x A$.
Case 1: $\deg A = \deg C$. We have $f(\infty) \neq \infty$ and thus $x \in K$, $C(x) = 0$ and $A(x) \neq 0$. Conversely any x with $C(x) = 0$ satisfies the equality $f(x) = \infty$. In this case we obtain

$$S_\infty = \sum_{x\in K: C(x)=0} (\mathrm{ord}_x C - 1) = \deg C - \deg \mathrm{rad} C = \deg A - \deg \mathrm{rad} C.$$

Case 2: $\deg A > \deg C$**.** This case is analogous but we have $f(\infty) = \infty$ and therefore we have to add the summand $e_\infty(f) - 1 = -\mathrm{ord}_\infty(A/C) - 1 = \deg A - \deg C - 1$. We have then $S_\infty = \deg A - \deg \mathrm{rad} C - 1$.
Putting everything together we get

$$S_\infty = \deg A - \deg \mathrm{rad} C - \epsilon \quad \text{with} \quad \epsilon = \begin{cases} 0 & : \deg A = \deg C, \\ 1 & : \deg A > \deg C. \end{cases} \tag{8.5}$$

We sum (8.3), (8.4), (8.5) and from (8.1) we obtain

$$\begin{aligned} 2\deg A - 2 &= \deg A - \deg \mathrm{rad} A + \deg B - \deg \mathrm{rad} B + \deg A - \deg \mathrm{rad} C - \epsilon + S \\ &= S + 3\deg A - \deg \mathrm{rad}(ABC) - \epsilon \end{aligned}$$

since A, B, C do not have any common root and by $\deg A = \deg B$.
It follows that $\deg A = \deg \mathrm{rad}(ABC) + \epsilon - 2 - S$. But $S \geq 0$ and $\epsilon \leq 1$. The claim follows from $\deg A = \max\{\deg A, \deg B, \deg C\}$. □

Remark 8.2.9. In the notation of the proof, we note that we have equality exactly when $\epsilon = 1$ and $S = 0$. The first is equivalent to $\deg A > \deg C$, and therefore to $f(\infty) = \infty$. The second implies that f is unramified at all points of $\mathbb{P}^1(K) \setminus f^{-1}(\{0, 1, \infty\})$.
This last fact will play an important role in the next section.

Definition 8.2.10. Let K be an algebraically closed field of characteristic 0 and $f \in K(X)$ is not constant. If f is unramified outside of $f^{-1}(\{0, 1, \infty\})$ we say that f is a **Belyĭ map**.

"Fermat's last Theorem" for polynomials is now easy to prove.

Corollary 8.2.11. *Let K be a field of characteristic 0 and $n \geq 3$ an integer. Let $A, B, C \in K[X] \setminus \{0\}$ without any common factor and with $A^n + B^n = C^n$. Then A, B, C are all constant.*

Proof. We may assume that K is algebraically closed. Assume by contradiction that we have $A, B, C \in K[X] \setminus \{0\}$ with $A^n + B^n = C^n$ where at least one between A, B, C in non-constant. Recall they are coprime. We may then use Theorem 8.2.3 with A^n, B^n and C^n.
We have $\mathrm{rad}(A^n B^n C^n) = \mathrm{rad}(ABC)$ and thus

$$n \max\{\deg A, \deg B, \deg C\} = \max\{\deg A^n, \deg B^n, \deg C^n\} \leq \deg \mathrm{rad}(ABC) - 1.$$

But $\deg \mathrm{rad} ABC \leq \deg(ABC) \leq 3 \max\{\deg A, \deg B, \deg C\}$. We have a contradiction for $n \geq 3$. □

8.3 Belyĭ's Lemma

Belyĭ's Lemma plays a central role in the proof of Theorem 8.1.7. In its most general formulation the lemma is a statement about algebraic curves which are defined over $\overline{\mathbb{Q}}$. We consider the case of the projective line $\mathbb{P}^1$. The general case follows reducing to this case.
We write $\overline{\mathbb{Q}}(X)$ for the field of rational functions over the algebraic numbers and we see its elements as maps $\mathbb{P}^1(\overline{\mathbb{Q}}) \to \mathbb{P}^1(\overline{\mathbb{Q}})$ as already done before. Two non-constant rational functions g and h can clearly be composed to get a rational function $h \circ g$.

Lemma 8.3.1 (Belyĭ). *Let $g \in \overline{\mathbb{Q}}(X) \setminus \overline{\mathbb{Q}}$ and let S be a finite set of points of $\mathbb{P}^1(\overline{\mathbb{Q}})$. There exists a non-constant rational function $h \in \mathbb{Q}(X)$, such that $f = h \circ g$ satisfies the following:*

(i) we have $f(S) \subset \{0, 1, \infty\}$

(ii) and f is unramified outside of $f^{-1}(\{0, 1, \infty\})$, i.e., f is a Belyĭ map.

Proof. We divide the proof into two parts.

Claim I: Let $S \subset \mathbb{C}$ be a finite set of algebraic numbers. There exists $P \in \mathbb{Q}[X] \setminus \mathbb{Q}$, such that $P(S) \subset \mathbb{Q}$ and $P\colon \mathbb{P}^1(\overline{\mathbb{Q}}) \to \mathbb{P}^1(\overline{\mathbb{Q}})$ is unramified outside of $P^{-1}(\mathbb{Q} \cup \{\infty\})$.

Proof of Claim I: The statement is stronger if we enlarge S. Therefore we are allowed to assume that S is closed under conjugation (i.e., if $\alpha \in S$ then all other roots of the minimal polynomial of α over $\mathbb{Q}$ are also in S).
We proceed by induction on $n = \#S$.
If $n \leq 1$, we have $S \subset \mathbb{Q}$ and we can choose $P = X$.
Let $n \geq 2$. Since every element of S is algebraic over $\mathbb{Q}$, it has a minimal polynomial over $\mathbb{Q}$. Two conjugate elements in S have the same minimal polynomial. The product of all the distinct minimal polynomials is a polynomial $P_1 \in \mathbb{Q}[X] \setminus \mathbb{Q}$ of degree n, such that $P_1(s) = 0$ for all $s \in S$. We can consider P_1 as a self-map $\mathbb{P}^1(\overline{\mathbb{Q}}) \to \mathbb{P}^1(\overline{\mathbb{Q}})$. Then P_1 is ramified at ∞ (since $\deg P_1 \geq 2$) and at all the roots of the derivative P_1'. If we set $S' = \{x \in \overline{\mathbb{Q}} : P_1'(x) = 0\}$, we have $\#S' \leq \deg P_1' = n - 1$ and therefore $\#S_1 \leq n - 1$ where $S_1 = P_1(S')$. Moreover, S_1 is stable under conjugation.
Now we apply the inductive hypothesis on S_1. There is $P_2 \in \mathbb{Q}[X] \setminus \mathbb{Q}$ such that $P_2(S_1) \subset \mathbb{Q} \cup \{\infty\}$ and so that P_2 is unramified outside $P_2^{-1}(\mathbb{Q} \cup \{\infty\})$.
We set $P = P_2 \circ P_1 \in \mathbb{Q}[X]$ and note that $\deg P = \deg P_2 \deg P_1 > 0$.
Every element of S is a root of P_1. We then have $P(S) = P_2(P_1(S)) = P_2(\{0\}) \subset \mathbb{Q}$.
Let $x \in \mathbb{P}^1(\overline{\mathbb{Q}})$ be a ramification point of $P_2 \circ P_1$. We must show that $P_2(P_1(x)) \in \mathbb{Q} \cup \{\infty\}$. Without loss of generality we may assume $x \neq \infty$. Then, the derivative of $P_2 \circ P_1$ vanishes at x. By the chain rule we have $P_2'(P_1(x))P_1'(x) = 0$, so $P_1'(x) = 0$ or $P_2'(P_1(x)) = 0$. In the first case we have $x \in S'$ by definition and then $P_2(P_1(x)) \in P_2(S_1) \subset \mathbb{Q} \cup \{\infty\}$. In the second case P_2 ramifies at $P_1(x)$, so $P_2(P_1(x)) \in \mathbb{Q} \cup \{\infty\}$ by the inductive hypothesis.
We are done proving Claim I. Next we show that we may replace $\mathbb{Q} \cup \{\infty\}$ by $\{0, 1, \infty\}$.

Claim II: Let $S \subset \mathbb{Q} \cup \{\infty\}$ be a finite set. There exists a non-constant rational function $f \in \mathbb{Q}(X)$ such that $f(S) \subset \{0, 1, \infty\}$ and such that $f\colon \mathbb{P}^1(\overline{\mathbb{Q}}) \to \mathbb{P}^1(\overline{\mathbb{Q}})$ is unramified outside $f^{-1}(\{0, 1, \infty\})$.

Proof of Claim II: Again we perform induction on $n = \#S$.
If $n \leq 3$ we may assume that $S = \{\alpha, \beta, \gamma\}$ with α, β, γ pairwise distinct (we may always add points to S, the result becomes stronger). If $S \subset \mathbb{Q}$ we set $f = \frac{\beta-\gamma}{\beta-\alpha}\frac{X-\alpha}{X-\gamma}$. Then we have $f(\alpha) = 0, f(\beta) = 1$ and $f(\gamma) = \infty$. If $S = \{\alpha, \beta, \infty\}$ we take $f = (X - \alpha)/(\beta - \alpha)$. Then, one can easily see that f does not ramify at any point of $\mathbb{P}^1(\overline{\mathbb{Q}})$.
Let $n \geq 4$ and $\alpha, \beta, \gamma, t \in S$ with $\alpha < t < \beta < \gamma$. As in the case $n \geq 3$ we consider $\ell = \frac{\beta-\gamma}{\beta-\alpha}\frac{X-\alpha}{X-\gamma}$ which is not ramified and $\ell(\{\alpha, \beta, \gamma\}) = \{0, 1, \infty\}$. Moreover we have

$\ell(t) = \frac{(\beta-\gamma)(t-\alpha)}{(t-\gamma)(\beta-\alpha)} \in (0,1)$. In the case $S = \{\alpha, t, \beta, \infty\}$ with $\alpha < t < \beta$ we take $\ell = (X-\alpha)/(\beta-\alpha)$. In any case, as rational function, ℓ is invertible so we may assume that $\{0, t, 1, \infty\} \subset S$ with $t \in (0,1)$ rational.
We write $t = a/(a+b)$ with $a, b \in \mathbb{Z}^{>0}$ and define

$$P_1 = \frac{(a+b)^{a+b}}{a^a b^b} X^a (1-X)^b \in \mathbb{Q}[X].$$

We see right away that $P_1(0) = P_1(1) = 0$, $P_1(\infty) = \infty$ and

$$P_1(t) = \frac{(a+b)^{a+b}}{a^a b^b} \frac{a^a}{(a+b)^a} \frac{b^b}{(a+b)^b} = 1.$$

Therefore, $P_1(\{0, t, 1, \infty\}) = \{0, 1, \infty\}$ and thus $P_1(S)$ has at most $n-1$ elements.
We now apply the inductive hypothesis on $P_1(S)$ and obtain f_1 such that $f_1(P_1(S)) \subset \{0, 1, \infty\}$ and such that f_1 is unramified outside $f_1^{-1}(\{0, 1, \infty\})$.
Finally, we surely have $f(S) = f_1(P_1(S)) \subset \{0, 1, \infty\}$. Let $x \in \mathbb{P}^1(\overline{\mathbb{Q}})$ be a ramification point of f. We must show that $f(x) \in \{0, 1, \infty\}$. We may assume $x \neq \infty$. As before we have $f_1'(P_1(x))P_1'(x) = 0$.
If $P_1'(x) = 0$ we consider

$$P_1' = \frac{(a+b)^{a+b}}{a^a b^b}(aX^{a-1}(1-X)^b - bX^a(1-X)^{b-1}) = (a-(a+b)X)\frac{P_1}{X(1-X)}.$$

If $x \neq t = (a+b)/b$, then $P_1(x) = 0$ and $P_1(t) = 1$ by construction. We then have $P_1(x) \in P_1(S)$ and thus $f(x) = f_1(P_1(x)) \in \{0, 1, \infty\}$.
If $f_1'(P_1(x)) = 0$ then f_1' ramifies at $P_1(x)$ and then $P_1(x) \in \{0, 1\} \subset P_1(S)$. It follows that $f(x) \in \{0, 1, \infty\}$.

We are now ready to finish the proof of the lemma.
We set $S_1 = \{x \in \mathbb{P}^1(\overline{\mathbb{Q}}) : g \text{ is ramified at } x\}$ and we apply Claim I to $g(S \cup S_1) \setminus \{\infty\}$. We obtain P.
We then define $S_2 = \{x \in \overline{\mathbb{Q}} : P'(x) = 0 \text{ and } P(x) \in \mathbb{Q}\} \cup \{\infty\}$ and $S_3 = P(g(S \cup S_1) \cup S_2)$. We apply Claim II to S_3 and obtain f_1.
The chain rule implies that $f = f_1 \circ P \circ g$ is unramified outside $f^{-1}(\{0, 1, \infty\})$ and $f(S) \subset \{0, 1, \infty\}$. □

Proof of Theorem 8.1.7. It is enough to consider the $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq 2$ and $\alpha \in \mathbb{R}$. Let $P \in \mathbb{Z}[X]$ be the unique integer irreducible polynomial with α as root and with positive leading coefficient. We consider it as a self-map of the projective line. We apply Belyĭ's Lemma to P and $S = \{\text{roots of } P\}$.
We obtain a rational map $f = h \circ P$ unramified outside $f^{-1}(\{0, 1, \infty\})$ and such that $f(S) = h(0) \subset \{0, 1, \infty\}$. After a linear transformation of the image, we may assume that $h(0) = 0$.
We write $f = A/C$ with $A, C \in \mathbb{Z}[X] \setminus \{0\}$ coprime. Let now $B \in \mathbb{Z}[X]$ with $A + B = C$.
We have $d = \deg f = \max\{\deg A, \deg C\}$.

We now homogenize the three polynomials A, B, C and obtain

$$A^{\hom}(X,Y) = Y^d A(X/Y), \quad B^{\hom}(X,Y) = Y^d B(X/Y), \quad C^{\hom}(X,Y) = Y^d C(X/Y)$$

with and $A^{\hom} + B^{\hom} = C^{\hom}$.
Let p/q be a good approximation of α with coprime $p \in \mathbb{Z}, q \in \mathbb{Z}^{>0}$, meaning $q^{2+\epsilon}|\alpha - p/q| \ll 1$, where $x \ll y$ for $x, y \in [0,\infty)$ means that $x \leq L \cdot y$ for some constant $L > 0$, independent of p/q. In particular we assume $|\alpha - p/q| \leq 1$.
The equality $A^{\hom}(p,q)B^{\hom}(p,q)C^{\hom}(p,q) = 0$ is satisfied by at most finitely many fractions p/q. We then are allowed to assume that this product is $\neq 0$. We define

$$m = \gcd(A^{\hom}(p,q), B^{\hom}(p,q), C^{\hom}(p,q))$$

and

$$a = \frac{A^{\hom}(p,q)}{m}, \quad b = \frac{B^{\hom}(p,q)}{m}, \quad c = \frac{C^{\hom}(p,q)}{m}$$

which are integers. We then have $a + b = c$ and $\gcd(a,b,c) = 1$.
If we let $g = B/C$, then, since $A + B = C$ we have $\deg g \leq d = \max\{\deg A, \deg C\}$. We use Lemma 5.2.7 on f and g and obtain

$$H(x)^d \ll H(f(x), g(x)) \ll H(C(x) : A(x) : B(x)),$$

for all $x \in \mathbb{P}^1(\overline{\mathbb{Q}})$. We now set $x = p/q$ and get

$$\begin{aligned}\max\{|p|,|q|\}^d &\ll H\left(C\left(\frac{p}{q}\right) : A\left(\frac{p}{q}\right) : B\left(\frac{p}{q}\right)\right) = H(a:b:c)\\ &= \max\{|a|,|b|,|c|\} = \frac{\max\{|A^{\hom}(p,q)|, |B^{\hom}(p,q)|, |C^{\hom}(p,q)|\}}{m},\end{aligned}$$

where we have used the fact that a, b, c are coprime integers. We note that $A^{\hom}$ is a homogeneous polynomial of degree at most d and it follows that $|A^{\hom}(p,q)| \ll \max\{|p|,|q|\}^d$. The same holds for B and C in place of A and we conclude

$$\max\{|p|,|q|\}^d \ll \frac{\max\{|p|,|q|\}^d}{m}.$$

Therefore

$$m \ll 1. \tag{8.6}$$

We now factor

$$A^{\hom} = a_0 P_1^{m_1} \cdots P_r^{m_r}, \quad B^{\hom} = b_0 P_{r+1}^{m_{r+1}} \cdots P_s^{m_s}, \quad C^{\hom} = c_0 P_{s+1}^{m_{s+1}} \cdots P_t^{m_t} \tag{8.7}$$

with $a_0, b_0, c_0 \in \mathbb{Z} \setminus \{0\}$ and $P_1, \ldots, P_r \in \mathbb{Z}[X,Y]$ irreducible and $m_i \in \mathbb{Z}^{>0}$.
A prime divisor of abc must divide $a_0 b_0 c_0$ or at least one of the values $P_i(p,q)$ for $1 \leq i \leq t$. Therefore, $\operatorname{rad}(abc) \mid a_0 b_0 c_0 P_1(p,q) \cdots P_t(p,q)$.

Recall that $f(\alpha) = 0$ and then $A(\alpha) = 0$. We may then assume that $P_1 = P(X/Y)Y^{\deg P_1}$ and $\deg P_1 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. As $|p| \ll q$ we have

$$\operatorname{rad}(abc) \leq |a_0 b_0 c_0 P_1(p,q) \cdots P_t(p,q)| \ll |P_1(p,q)| q^D \tag{8.8}$$

with

$$D := \sum_{i=2}^{t} \deg P_i = -[\mathbb{Q}(\alpha) : \mathbb{Q}] + \sum_{i=1}^{t} \deg P_i. \tag{8.9}$$

Since $B(\alpha) \neq 0$ and we may assume $|\alpha - p/q|$ to be arbitrarily small, by continuity we have $|B(p/q)| \gg 1$ and thus we have $|B^{\hom}(p,q)| = q^d |B(p/q)| \gg q^d$ where we recall $d = \deg f$. This implies $|b| \gg \frac{q^d}{m}$ and by (8.6) we have

$$|b| \gg q^d.$$

We now apply the *abc*-conjecture. By (8.8) it follows that $q^d \ll \max\{|a|, |b|, |c|\} \ll (|P_1(p,q)| q^D)^{1+\epsilon}$ and therefore

$$|P(p/q) q^{[\mathbb{Q}(\alpha):\mathbb{Q}]}| = |P_1(p,q)| \gg q^{d - D - d\epsilon/(1+\epsilon)}.$$

Recall that $P(\alpha) = 0$. Then,

$$\frac{|P(p/q) - P(\alpha)|}{|p/q - \alpha|} \ll |P'(\alpha)| \ll 1,$$

as $p/q \to \alpha$.
Therefore, we have $|P(p/q)| \ll |\alpha - p/q|$ and thus

$$\left| \alpha - \frac{p}{q} \right| \gg q^{d - D - [\mathbb{Q}(\alpha):\mathbb{Q}] - d\epsilon/(1+\epsilon)}. \tag{8.10}$$

Finally we want to show that $d - D - [\mathbb{Q}(\alpha) : \mathbb{Q}] = -2$. We use the Riemann–Hurwitz formula, Theorem 8.2.8, on f. Recall that f is unramified outside $f^{-1}(\{0, 1, \infty\})$. Therefore, only points $x \in \mathbb{P}^1(\overline{\mathbb{Q}})$ with $f(x) = 0, 1, \infty$ play a role in the formula. Anyone of such points is a root of one between A, B and C. Then,

$$2d - 2 = \sum_{i=1}^{t} (m_i - 1) \deg P_i.$$

Each polynomial between $A^{\hom}, B^{\hom}$ and $C^{\hom}$ has degree d. Therefore

$$3d = \deg(A^{\hom} C^{\hom} B^{\hom}) = \sum_{i=1}^{t} m_i \deg P_i$$

by (8.7).

Taking the difference between the last two equalities we see that

$$d + 2 = \sum_{i=1}^{t} \deg P_i = D + [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

by (8.9). In other words, $d - D - [\mathbb{Q}(\alpha) : \mathbb{Q}] = -2$. By (8.10) it follows now that

$$\left| \alpha - \frac{p}{q} \right| \gg q^{-2-d\epsilon/(1+\epsilon)}.$$

This is exactly the claim of Roth's Theorem, after an appropriate modification of ϵ. $\square$

Index

Bibliography

[1] F. Barroero, *AL420 - Algebraic Number Theory*, Lecture notes, 2020.

[2] E. Bombieri, D. Masser and U. Zannier, *Intersecting a curve with algebraic subgroups of multiplicative groups*, Int. Math. Res. Notices 20 (1999), 1119–1140.

[3] I. Gelfand, M. Kapranov, A. Zelevinsky, *Discriminants, Resultants, and Multidimensional Determinants*

[4] D. Marcus, *Number fields*. Universitext, Springer, Cham, 2018.

[5] Milne, J.S. *Fields and Galois Theory*, Lecture notes available at https://www.jmilne.org/math/CourseNotes/ft.html

[6] J. Neukirch, *Algebraic Number theory*. Grundlehren der Mathematischen Wissenschaften, 322, Springer-Verlag, Berlin, 1991.

[7] P. Samuel, *Algebraic Theory Of Numbers*. Translated from the French by A.J. Silberger Houghton Mifflin Co., Boston, Mass. 1970.

[8] R. Schoof, *Algebraic Number Theory*. Dispense disponibili al link: http://www.mat.uniroma2.it/~eal/moonen.pdf

[9] J. Silverman, *The Arithmetic Of Dynamical Systems*, GTM 241.

[10] U. Zannier, *Lecture Notes on Diophantine Analysis*