Diophantine Approximation

Lukas Pottmeyer

January 17, 2022

Preface

These lecture notes were written during the Corona-term 2020. There are surely still plenty of typos, although already many have been found by the participants of this course. I thank all of the participants for their interest in the topic and their hunt for typos, errors and inaccuracies! If you notice further issues, please sent me a mail.
Many sources have been used to write these notes, and I often follow the outline of some sections from other books quite closely. This includes:

- The presentation of the theory of continued fractions roughly follows the presentation in [11].
- Everything on Siegel's Lemma is essentially taken from [5].
- The proof of Dobrowolski's theorem closely follows the outline from [8].
- the proof of Roth's Lemma is a mixture from the proofs given in [1] and [5].
- The proof of Roth's theorem closely follows the outline in [1].
- The proof of the Gelfond-Schneider theorem is essentially taken from [9].
- The mentioned applications of linear forms in logarithms are taken from [3].

Notations

$\mathbb{Z}$	the integers
$\mathbb{Q}$	the rational numbers
$\mathbb{R}$	the real numbers
$\mathbb{C}$	the complex numbers
$\mathbb{N}$	the positive integers $\{1, 2, 3, \ldots\}$
$\mathbb{N}_0$	the non-negative integers $\{0, 1, 2, 3, \ldots\}$
$\overline{\mathbb{Q}}$	a fixed algebraic closure of $\mathbb{Q}$ contained in $\mathbb{C}$
$\lfloor \alpha \rfloor$	the Gauß-bracket of α (largest integer smaller or equal to the real number α)
$\mathbf{\{}\alpha\mathbf{\}}$	the fractional part of α ($\alpha - \lfloor \alpha \rfloor$)
$\lvert z \rvert$	the usual absolute value of $z \in \mathbb{C}$
$\lvert M \rvert$	the cardinality of the set M
$M(\alpha)$	the Mahler measure of $\alpha \in \overline{\mathbb{Q}}$
K_v	the completion of the number field K with respect to the absolute value v on K
d_v	the local degree $[K_v : \mathbb{Q}_p]$
M_K	set of pairwise non equivalent non-trivial absolute values v on the number field K, normalized such that the restriction of an archimedean v to $\mathbb{Q}$ is the usual $\lvert . \rvert$, and the restriction of a non-archimedean v to $\mathbb{Q}$ is a usual p-adic absolute value
$\mathcal{O}_K$	the ring of integers of a number field K
$H(\alpha)$	the absolute multiplicative Weil-height of $\alpha \in \overline{\mathbb{Q}}$
$h(\alpha)$	the absolute logarithmic Weil-height of $\alpha \in \overline{\mathbb{Q}}$

Contents

1 Foundations **1**
- 1.1 Introduction to Diophantine Approximations . . . 1
- 1.2 Finite Continued Fractions . . . 8
- 1.3 Infinite Continued Fractions . . . 12
- 1.4 Periodic Continued Fractions and Pell's Equation . . . 21

2 The Weil-Height **27**
- 2.1 The Mahler Measure . . . 27
- 2.2 Recap on Valuation Theory . . . 40
- 2.3 The Weil-height (finally) . . . 47
- 2.4 Siegel's Lemma . . . 54
- 2.5 On Lehmer's Conjecture . . . 62
- 2.6 Siegel's Lemma Once More . . . 67

3 Roth's Theorem **73**
- 3.1 Thue equations . . . 74
- 3.2 Preliminaries I – Multivariable Polynomial Estimates . . . 80
- 3.3 Preliminaries II – Linearly Independent Polynomials . . . 85
- 3.4 Preliminaries III – Roth's Lemma . . . 90
- 3.5 The Proof . . . 95
- 3.6 Generalizations . . . 104

4 Linear Forms in Logarithms **115**
- 4.1 The Gelfond-Schneider Theorem . . . 115
- 4.2 Applications . . . 124

Chapter 1

Foundations

1.1 Introduction to Diophantine Approximations

The word *Diophantine* usually refers to the integers or rationals. Hence, the main goal in the field of Diophantine Approximation is to approximate real numbers by rational numbers. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, this is always possible to an arbitray accuracy. However, some approximations are *nicer* than others. For instance[1]

$$\begin{aligned} \pi = 3,1415926\ldots &\approx \frac{314159}{100000} && \text{(“good approximation with huge denominator”)} \\ &\approx \frac{355}{113} && \text{(“better approximation with small denominator”)} \end{aligned}$$

So, in some intuitive way, the latter approximation is much nicer.
Formally, for a given $\alpha \in \mathbb{R}$, we want to study $\frac{p}{q} \in \mathbb{Q}$, with $p \in \mathbb{Z}$, $q \in \mathbb{N}$, and $\gcd(p,q) = 1$, such that $|\alpha - \frac{p}{q}|$ is small. This is surely the case if $|q\alpha - p|$ is small. Hence, we will frequently work with this latter quantity.

Definition 1.1.1. For $\alpha \in \mathbb{R}$ we define the *Gauß-bracket of* α as the largest integer $\lfloor \alpha \rfloor$ smaller or equal to α. The *fractional part of* α is $\{\alpha\} = \alpha - \lfloor \alpha \rfloor$.

Remark 1.1.2. The function $\lfloor \cdot \rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$ is also known as the *floor function*. To be able to distinguish between the fractional part of α and the set with the only element α (although it should always be clear from the context), we put the brackets of the fractional part in bold face.
Note that we always have $\{\alpha\} \in [0,1)$ for all $\alpha \in \mathbb{R}$.

Example 1.1.3. It is

- $\lfloor \pi \rfloor = 3$ and $\{\pi\} = 0,1415926\ldots$
- $\left\lfloor \frac{3}{4} \right\rfloor = 0$ and $\{\frac{3}{4}\} = \frac{3}{4}$
- $\lfloor -e \rfloor = \lfloor -2,7182\ldots \rfloor = -3$ and $\{-e\} = -e + 3 = 0,2817\ldots$

[1] the first few digits of π can be remembered by: *How I want a drink? Alcoholic of course!* (just count the letters of each word)

Lemma 1.1.4. *Let $\alpha = \frac{a}{b} \in \mathbb{Q}$, with $a \in \mathbb{Z}$, $b \in \mathbb{N}$, and $\gcd(a,b) = 1$. Let $p, q \in \mathbb{Z}$ such that $\alpha \neq \frac{p}{q}$, then $|q\alpha - p| \geq \frac{1}{b}$.*

Proof. This is trivial: We have $|qa - pb| = 0$ if and only if $\alpha = \frac{a}{b} = \frac{p}{q}$. If this is not the case, we have

$$|q\alpha - p| = \left| q\frac{a}{b} - p \right| \geq \frac{|qa - pb|}{b} \geq \frac{1}{b}.$$

□

Notation 1.1.5. Usually, when speaking of a rational number $\frac{p}{q}$, we mean that $p \in \mathbb{Z}$, $q \in \mathbb{N}$, and $\gcd(p,q) = 1$.

Theorem 1.1.6 (Dirichlet)**.** *Let $\alpha \in \mathbb{R}$ be arbitrary. For each $Q \in \mathbb{N}$, there are coprime $p, q \in \mathbb{Z}$, with $q \in \{1, \ldots, Q\}$, such that*

$$|q\alpha - p| < \frac{1}{Q}. \tag{1.1}$$

Proof. The following proof is most beautiful! We cut the interval $[0,1)$ into Q subintervals of equal size; i.e.

$$[0,1) = \underbrace{[0, \frac{1}{Q})}_{=:I_1} \cup \underbrace{[\frac{1}{Q}, \frac{2}{Q})}_{=:I_2} \cup \ldots \cup \underbrace{[\frac{Q-1}{Q}, 1)}_{=:I_Q}.$$

The $Q+1$ numbers $\{0 \cdot \alpha\}$, $\{1 \cdot \alpha\}$, …, $\{Q \cdot \alpha\}$ all lie in $[0,1)$. Now, we have $Q+1$ numbers in Q subintervals, and it follows that two of these numbers must lie in the same subinterval. Say $\{a \cdot \alpha\}, \{b \cdot \alpha\} \in I_k$, for $a, b, \in \{1, \ldots, Q\}$, $k \in \{1, \ldots, Q\}$, and $a > b$. Then

$$\begin{aligned} \frac{1}{Q} > |\{a \cdot \alpha\} - \{b \cdot \alpha\}| &= |a \cdot \alpha - b \cdot \alpha - \lfloor a \cdot \alpha \rfloor + \lfloor b \cdot \alpha \rfloor| \\ &= |(a-b) \cdot \alpha - (\lfloor a \cdot \alpha \rfloor - \lfloor b \cdot \alpha \rfloor)|. \end{aligned}$$

Hence, (1.1) is fulfilled with $q = a - b \in \{1, \ldots, Q\}$ and $p = \lfloor a \cdot \alpha \rfloor - \lfloor b \cdot \alpha \rfloor \in \mathbb{Z}$. □

Corollary 1.1.7. *A real number $\alpha \in \mathbb{R}$ is irrational (i.e. $\in \mathbb{R} \setminus \mathbb{Q}$) if and only if there are sequences $(p_n)_{n \in \mathbb{N}} \in \mathbb{Z}$ and $(q_n)_{n \in \mathbb{N}} \in \mathbb{N}$, such that*

$$0 \neq |q_n\alpha - p_n| \longrightarrow 0 \text{ as } n \text{ tends to infinity.} \tag{1.2}$$

Proof. If α is irrational, then surely $|q\alpha - p| \neq 0$ for all $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. By Theorem 1.1.6, for any $n \in \mathbb{N}$, we can find $p_n \in \mathbb{Z}$ and $q_n \in \mathbb{N}$, such that $|q_n\alpha - p_n| < \frac{1}{n}$. Hence, (1.2) follows. If on the other hand α is rational, then (1.2) is not satisfied by Lemma 1.1.4. □

Slogan: Irrational numbers can be better approximated than rational numbers!

Example 1.1.8. We give two applications:

(a) We have $\left\lfloor \sqrt{2} \right\rfloor = 1$ (since $1^2 < 2$ and $2^2 > 2$). Hence, $\left| \sqrt{2} - 1 \right| < 1$. It follows that $0 \neq \left| (\sqrt{2}-1)^n \right|$ tends to zero as n tends to infinity. Since $(\sqrt{2}-1)^n \in \mathbb{Z}[\sqrt{2}]$, for any $n \in \mathbb{N}$, there are $p_n, q_n \in \mathbb{Z}$ such that $(\sqrt{2}-1)^n = q_n\sqrt{2} - p_n$. This means that (1.2) is satisfied, and therefore $\sqrt{2}$ is irrational. We all knew this before, but this proof does not need any knowledge of prime decomposition!

If you like to have it slightly more explicit, one can show that

- $p_0 = -1$, $p_1 = 1$, $p_2 = -3$, and $p_{n+1} = -2p_n + p_{n-1}$ for all $n \geq 2$
- $q_0 = 0$, $q_1 = 1$, $p_2 = -2$, and $q_{n+1} = -2q_n + q_{n-1}$ for all $n \geq 2$.

(b) Euler's constant e equals $\sum_{i=0}^{\infty} \frac{1}{i!}$. Set $q_n = n! \in \mathbb{N}$ and $p_n = n! \cdot \sum_{i=0}^{n} \frac{1}{i!} \in \mathbb{N}$. Then, it is

$$\begin{aligned} 0 \neq |q_n e - p_n| &= n! \cdot \sum_{i=1}^{\infty} \frac{1}{(n+i)!} \\ &= \sum_{i=1}^{\infty} \frac{1}{(n+1)(n+2)\cdot\ldots\cdot(n+i)} < \sum_{i=1}^{\infty} \frac{1}{(n+1)^i} \\ &= \frac{1}{1-\frac{1}{n+1}} - 1 = \frac{1}{n} \overset{n\to\infty}{\longrightarrow} 0. \end{aligned}$$

By Corollary 1.1.7 it follows that e is irrational.

The next corollary to Theorem 1.1.6 is the first major result of Diophantine Approximation, that we come across.

Corollary 1.1.9. *Let $\alpha \in \mathbb{R}$ be irrational. There are infinitely many rational numbers $\frac{p}{q}$, with $\gcd(p,q) = 1$, $q \geq 1$, such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{1.3}$$

Proof. Actually, the proof is almost immediately clear from Theorem 1.1.6. But as the result is that important, we will give the proof in full detail.
Assume that for some irrational α there are only finitely many – say precisely n – rational numbers $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ satisfying (1.3). Since $\alpha \notin \mathbb{Q}$, we have $0 \neq \left|\alpha - \frac{p_i}{q_i}\right|$ for all $i \in \{1, \ldots, n\}$. Take any $Q \in \mathbb{N}$ satisfying $\frac{1}{Q} < \min_{i\in\{1,\ldots,n\}} \left|\alpha - \frac{p_i}{q_i}\right|$. By Theorem 1.1.6, there are coprime $p, q \in \mathbb{Z}$, with $q \in \{1, \ldots, Q\}$, such that

$$0 \neq \left|\alpha - \frac{p}{q}\right| = \frac{1}{q} \cdot |q\alpha - p| < \frac{1}{qQ} < \left|\alpha - \frac{p_i}{q_i}\right| \qquad \forall\, i \in \{1, \ldots, n\}.$$

In particular, $\frac{p}{q} \neq \frac{p_i}{q_i}$ for all $i \in \{1, \ldots, n\}$. Moreover, as $q \in \{1, \ldots, Q\}$, we have

$$\left|\alpha - \frac{p}{q}\right| = \frac{1}{q} \cdot |q\alpha - p| < \frac{1}{qQ} \leq \frac{1}{q^2}.$$

So, there are at least $n+1$ rational numbers satisfying (1.3), which contradicts our assumption. Hence, there must be infinitely many rational numbers satisfying (1.3). This proves the corollary. □

Remark 1.1.10. The exponent 2 in (1.3) will keep us busy for some time . A natural question is, whether the statement of Corollary 1.1.9 remains true if 2 is replaced by 3, or 4, or 5, ... Note that increasing the exponent makes the approximations better!

Notation 1.1.11. Throughout the lectures, we will fix an algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and denote it by $\overline{\mathbb{Q}}$. An element in $\alpha \in \overline{\mathbb{Q}}$ is called *algebraic* or an *algebraic number*. This means, that there are integers $a_0, \ldots, a_d$, with $a_d \neq 0$, such that $a_d\alpha^d + a_{d-1}\alpha^{d-1} + \ldots + a_0 = 0$.

A different way to formulate this, is that there is a polynomial $f(x) \in \mathbb{Z}[x] \setminus \{0\}$, with $f(\alpha) = 0$. In fact, there is a unique (up to multiplication by -1) irreducible polynomial $f(x) \in \mathbb{Z}[x]$ satisfying $f(\alpha) = 0$. Such a polynomial is called *minimal polynomial of* α. If $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_d$ is the minimal polynomial of α, then $k = \gcd(a_d, \ldots, a_0) = 1$, since otherwise $f(x) = k \cdot (\frac{a_d}{k}x^d + \ldots + \frac{a_0}{k})$ would not be irreducible.
An equivalent definition for an algebraic number is, that $\alpha \in \mathbb{C}$ is algebraic if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is finite. In this case, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ equals the degree of the minimal polynomial of α, and is called the *degree of* α.
You have learned all of this in your Algebra class, to which we refer for further details!

Theorem 1.1.12 (Liouville)**.** *Let $\alpha \in \overline{\mathbb{Q}}$ be of degree $d \geq 2$ (i.e. an algebraic irrational number). Then there is a constant $c(\alpha) > 0$ such that for all rational numbers $\frac{p}{q}$, $q \in \mathbb{N}$, we have $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$.*

Proof. We will present an analytic proof here. Later we will present an algebraic proof as well.
Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0$ be the minimal polynomial of α. Since $d \geq 2$, there is a non-constant polynomial $g(x) \in \mathbb{C}[x]$ such that $f(x) = (x - \alpha) \cdot g(x)$. Since any irreducible polynomial over $\mathbb{Z}[x]$ is separable (does not have multiple roots), we know that $g(\alpha) \neq 0$. Also, since $f(x)$ is irreducible, it has no roots in $\mathbb{Q}$, and hence $g(\frac{p}{q}) \neq 0$. Moreover, as a polynomial, $g(x)$ is a continuous self-map on $\mathbb{C}$. Let $\varepsilon > 0$ be smaller than the distance of α to any other root of $f(x)$. Then, $g(\beta) \neq 0$ for all $\beta \in \mathbb{C}$, with $|\alpha - \beta| < \varepsilon$. So in particular $0 \neq \delta = \sup_{|\alpha-\beta|<\varepsilon} |g(\beta)|$. Since $g(x)$ is continuous on $\mathbb{C}$, we also know that $\delta \neq \infty$. Hence, $c(\alpha) := \min\{\varepsilon, \delta^{-1}\} \in \mathbb{R}$.
Assume there are $p \in \mathbb{Z}$, $q \in \mathbb{N}$, such that $\left|\alpha - \frac{p}{q}\right| \leq \frac{c(\alpha)}{q^d}$. Then

$$\begin{aligned} \left|\alpha - \frac{p}{q}\right| < \varepsilon \implies 0 \neq \left|g(\frac{p}{q})\right| < \delta \\ \implies \left|f(\frac{p}{q})\right| = \left|\alpha - \frac{p}{q}\right| \cdot \left|g(\frac{p}{q})\right| < \frac{c(\alpha)}{q^d} \cdot \delta \leq \frac{1}{q^d}. \end{aligned}$$

Multiplying both sides of the latter inequality by q^d yields

$$\begin{aligned} 1 &> \left|q^d \cdot f(\frac{p}{q})\right| \\ &= \left|q^d \cdot (a_d(\frac{p}{q})^d + a_{d-1}(\frac{p}{q})^{d-1} + \ldots + a_0\right| = \left|a_d p^d + a_{d-1}p^{d-1}q + \ldots + a_0 q^d\right| \in \mathbb{N}_0. \end{aligned}$$

It follows that $\left|q^d \cdot f(\frac{p}{q})\right| = 0$, which contradicts $f(\frac{p}{q}) \neq 0$. □

Remark 1.1.13. Theorem 1.1.12 tells us, that algebraic numbers cannot have "arbitrarily good" approximations. So maybe we can use this to prove the transcendence of certain complex numbers. Recall that an $\alpha \in \mathbb{C}$ is called *transcendental over* $\mathbb{Q}$ if it is not algebraic. Cantor provided a remarkable argument for the existence of transcendental numbers: The set of complex numbers is uncountable by Cantor's diagonal argument. On the other hand $\overline{\mathbb{Q}}$ consists of roots of polynomials in $\mathbb{Z}[x]$. We have

$$\mathbb{Z}[x] = \bigcup_{N=0}^{\infty} \{a_0 + a_1 x + \ldots + a_d x^d | d \in \mathbb{N}, a_0, \ldots, a_n \in \mathbb{Z}, \text{ and } d + |a_0| + \ldots + |a_d| = N\}.$$

As a countable union of finite sets, $\mathbb{Z}[x]$ is countable. But similarly,

$$\overline{\mathbb{Q}} = \bigcup_{f(x)\in\mathbb{Z}[x]} \{\alpha \in \mathbb{C} | f(\alpha) = 0\}$$

is a countable union of finite sets, and also countable. This means that the number of algebraic numbers in $\mathbb{C}$ is countable, and the number of transcendental elements in $\mathbb{C}$ is uncountable. So the probability that an randomly chosen $\alpha \in \mathbb{C}$ is transcendental is 1. However, the task of proving that a complex number is transcendental is extremely hard, and in most cases even impossible with the known methods.

Corollary 1.1.14. *Let α be a real number. If for all $d \in \mathbb{N}$ there are sequences $(p_n)_{n\in\mathbb{N}}$ in $\mathbb{Z}$ and $(q_n)_{n\in\mathbb{N}}$ in $\mathbb{N}$, such that*

$$0 \neq q_n^d \, |q_n\alpha - p_n| \longrightarrow 0 \ , \ as \ n \to \infty, \tag{1.4}$$

then α is transcendental.

Proof. We will show that if α is algebraic (i.e. not transcendental), then for some $d \in \mathbb{N}$ there are no such sequences satisfying (1.4). This is obvious for $\alpha \in \mathbb{Q}$ (see Lemma 1.1.4). Hence, we assume that α is algebraic of degree $d+1 \geq 2$. Then by Theorem 1.1.12, there is a positive constant $c(\alpha)$, such that $\left|\alpha - \frac{p}{q}\right| \geq \frac{c(\alpha)}{q^{d+1}}$ for all $p \in \mathbb{Z}$, $q \in \mathbb{N}$. This means precisely

$$q^d \cdot |q\alpha - p| > c(\alpha) \qquad \forall \ p \in \mathbb{Z}, \ q \in \mathbb{N}.$$

In particular, there are no sequences $(p_n)_{n\in\mathbb{N}}$ in $\mathbb{Z}$ and $(q_n)_{n\in\mathbb{N}}$ in $\mathbb{N}$, satisfying (1.4). This is what we needed to prove. □

Slogan: Transcendental numbers can be better approximated than algebraic numbers!

Example 1.1.15. The number $\alpha = 0,1\underbrace{00000\ldots0}_{n\text{-times}}1$ can be approximated by $\frac{1}{10}$ to a very high accuracy (depending on n). To construct a number α such that for any $n \in \mathbb{N}$ there is a rational number $\frac{p}{q}$ that satisfies $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}$, we may increase the numbers of zeros in the decimal digits between non-zero entries:

$$\alpha = 0,10\ldots010\ldots\ldots010\ldots\ldots\ldots010\ldots\ldots\ldots$$

Let's do this with a concrete example. We set

$$L := \sum_{k=1}^{\infty} \frac{1}{10^{k!}}.$$

The sum surely converges, so L is indeed a real number. For any $n \in \mathbb{N}$ we define $p_n = \sum_{k=1}^{n} 10^{n!-k!}$, and $q_n = 10^{n!}$ so that

$$s_n = \sum_{k=1}^{n} \frac{1}{10^{k!}} = \frac{\sum_{k=1}^{n} 10^{n!-k!}}{10^{n!}} = \frac{p_n}{q_n}.$$

For $d \in \mathbb{N}$ arbitrary, we have

$$\begin{aligned} 0 \neq q_n^d \cdot |q_n L - p_n| &= 10^{n!d} \left| 10^{n!} \sum_{k=1}^{\infty} \frac{1}{10^{k!}} - \sum_{k=1}^{n} 10^{n!-k!} \right| \\ &= 10^{n!d} \sum_{k=n+1}^{\infty} \frac{1}{10^{k!}} < 10^{n!d} \sum_{k=(n+1)!}^{\infty} \frac{1}{10^k} \\ &= \frac{1}{9 \cdot 10^{n!(n+1-d)} - 1} \overset{n\to\infty}{\longrightarrow} 0. \end{aligned}$$

It follows from Corollary 1.1.14, that L is transcendental. The number L is called the Liouville-constant. It was the first example of a transcendental number. Actually, this example was also the first proof of the existence of transcendental numbers, as its construction precedes Cantors set theoretic argument.

Remark 1.1.16. We want to compare Theorem 1.1.12 (which gives an lower bound for approximations of algebraic numbers) and Corollary 1.1.9 (which gives an upper bound for approximations of any real number). Therefore, let α be a real algebraic number of degree $d \geq 2$. As usual, all rational numbers $\frac{p}{q}$ are of the form $p \in \mathbb{Z}$, $q \in \mathbb{N}$, and $\gcd(p, q) = 1$. Then

$$\frac{c(\alpha)}{q^d} \underbrace{<}_{\text{for all rationals}} \left| \alpha - \frac{p}{q} \right| \underbrace{<}_{\text{for infinitely many rationals}} \frac{1}{q^2}.$$

Which of the two bounds is closer to the truth? It follows that if α is an irrational quadratic number (i.e. the degree d of α is two), then we can neither increase the exponent in Dirichlet's result, nor shrink the exponent in Liouville's result. Since, the exponent in Dirichlet's result is independent on α, we cannot improve this result, by replacing the exponent 2 by 3. This answers the question in Remark 1.1.10. After Liouville, many mathematicians tried to improve his result.

1844: $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}$ (Liouville)

1908: $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha,\varepsilon)}{q^{1+d/2+\varepsilon}} \quad \forall\, \varepsilon > 0$ (Thue)

1921: $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^{2\sqrt{d}}}$ (Siegel)

1947: $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^{\sqrt{2d}}}$ (Dyson)

Finally, in 1955 Klaus Friedrich Roth proved the following Theorem. This Theorem is best possible, since it is false for $\varepsilon = 0$ (if $d \geq 3$), by Dirichlet's Corollary 1.1.9. For his proof, Roth was awarded the Fields medal in 1958.

Theorem 1.1.17 (Roth's Theorem)**.** *For any $\varepsilon > 0$ and any $\alpha \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$, there exists a constant $c(\alpha, \varepsilon) > 0$, such that for all rational numbers $\frac{p}{q}$, $q \in \mathbb{N}$, we have $\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha,\varepsilon)}{q^{2+\varepsilon}}$.*

The goals for this course are:

- Prove how to find the "best" approximations for a given $\alpha \in \mathbb{R}$ (and explain what this actually means).
- We can also approximate real numbers by elements from a fixed number field. We will formulate and prove generalizations of all results from this introduction in this setting.
- We could replace the usual absolute value $|.|$ by a p-adic absolute value. We will study this setting as well.
- Finally, we aim to formulate and prove Roth's theorem for arbitrary absolute values and arbitrary number fields.

Exercises

Exercise 1.1. Let $n, Q \in \mathbb{N}$ be arbitrary. Prove that for every choice of n real numbers $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ there exist $p_1, \ldots, p_n \in \mathbb{Z}$ and $q \in \{1, \ldots, Q^n\}$ such that

$$|q\alpha_i - p_i| < \frac{1}{Q} \qquad \forall\, i \in \{1, \ldots, n\}.$$

Exercise 1.2. Improve Theorem 1.1.6 in the following way: Prove that for every $\alpha \in \mathbb{R}$ and every $Q \in \mathbb{N}$, there exist $p \in \mathbb{Z}$ and $q \in \{1, \ldots, Q\}$ such that $|q\alpha - p| \leq \frac{1}{Q+1}$.
Hint: Follow the original proof, with $Q + 1$ subintervals.

Exercise 1.3. Prove the claim in Example 1.1.8 (a). This is, prove that for

- $p_0 = -1$, $p_1 = 1$, $p_2 = -3$, and $p_{n+1} = -2p_n + p_{n-1}$ for all $n \geq 2$, and
- $q_0 = 0$, $q_1 = 1$, $p_2 = -2$, and $q_{n+1} = -2q_n + q_{n-1}$ for all $n \geq 2$

we have $(\sqrt{2} - 1)^n = q_n\sqrt{2} - p_n$ for all $n \in \mathbb{N}_0$.

Exercise 1.4. Give examples of at least five transcendental numbers, not including the Liouville-constant. Choose your examples such that you could prove of at least two of your examples that they are indeed transcendental.

Exercise 1.5. Prove that at least one of the numbers $\pi + e$ and $\pi \cdot e$ is transcendental.
Hint: You have to use some basic statements from an algebra course.

Exercise 1.6. Prove that the following real number is transcendental:

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{2^{3^k}}.$$

Hint: You may (and should) assume the validity of Roth's theorem.

1.2 Finite Continued Fractions

Definition 1.2.1. Let $x_0, x_1, \ldots, x_n \in \mathbb{R}$, with $x_1, \ldots, x_n > 0$. Then we set

$$\langle x_0, x_1, \ldots, x_n \rangle = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{\ddots + \cfrac{1}{x_{n-1} + \cfrac{1}{x_n}}}}}$$

If $a_0 \in \mathbb{Z}$ and $a_1, \ldots, a_n \in \mathbb{N}$, then $\langle a_0, \ldots, a_n \rangle$ is called a *finite continued fraction.*

So for instance

$$\langle 1, 2, 3 \rangle = 1 + \cfrac{1}{2 + \cfrac{1}{3}} = 1 + \frac{1}{\frac{7}{3}} = 1 + \frac{3}{7} = \frac{10}{7}.$$

Note that $\langle x_0, x_1, \ldots, x_n \rangle$ is always a real number, since $x_1, \ldots, x_n > 0$ and hence all denominators are (as sums of positive real numbers) positive.

Lemma 1.2.2. *For all $x_0, \ldots, x_n \in \mathbb{R}$, with $x_1, \ldots, x_n > 0$, we have*

(i) $\langle x_0, \ldots, x_n \rangle = x_0 + \frac{1}{\langle x_1, \ldots, x_n \rangle} = \langle x_0, \langle x_1, \ldots, x_n \rangle \rangle$.

(ii) $\langle x_0 + x, x_1, \ldots, x_n \rangle = x + \langle x_0, \ldots, x_n \rangle$ *for all* $x \in \mathbb{R}$.

(iii) $\langle x_0, x_1, \ldots, x_n \rangle = \langle x_0, x_1, \ldots, x_{n-2}, x_{n-1} + \frac{1}{x_n} \rangle$.

(iv) $\langle x_0, \ldots, x_n \rangle \geq x_0$ *with equality, if and only if* $n = 0$.

Proof. All these statements follow immediately from the definition. □

It is clear that any finite continued fraction represents a rational number. The converse is also true:

Proposition 1.2.3. *For every $\alpha \in \mathbb{Q}$, there are $a_0 \in \mathbb{Z}$ and $a_1, \ldots, a_n \in \mathbb{N}$ such that $\alpha = \langle a_0, \ldots, a_n \rangle$.*

Proof. The proof is constructive! Write $\alpha = \frac{p}{q}$, with $p \in \mathbb{Z}$, $q \in \mathbb{N}$, and $\gcd(p, q) = 1$. We run the Euclidean algorithm and get

$$\begin{aligned}
p &= a_0 q + r_0; && a_0 = \left\lfloor \frac{p}{q} \right\rfloor \in \mathbb{Z},\ r_0 \in \{0, \ldots, q-1\} \\
q &= a_1 r_0 + r_1; && a_1 \in \mathbb{N},\ r_1 \in \{0, \ldots, r_0 - 1\} \\
r_0 &= a_2 r_1 + r_2; && a_2 \in \mathbb{N},\ r_2 \in \{0, \ldots, r_1 - 1\} \\
&\vdots \\
r_{n-3} &= a_{n-1} r_{n-2} + r_{n-1}; && a_{n-1} \in \mathbb{N},\ r_{n-1} = 1 \text{ (since } \gcd(p, q) = 1) \\
r_{n-2} &= a_n r_{n-1}; && a_n = r_{n-2} \in \mathbb{N}
\end{aligned}$$

The remainders become smaller and smaller, so in particular $r_0, \dots, r_{n-1} \geq 1$. We claim that $\alpha = \frac{p}{q} = \langle a_0, \dots, a_n \rangle$ and prove this by induction on n.
If $n = 0$, then $p = a_0 q$ which implies $\alpha = \frac{p}{q} = a_0 = \langle a_0 \rangle$. This provides the induction base. Now we assume that the statement is correct whenever the Euclidean algorithm takes $n-1$ steps, which is the case for q and r_0. Hence, our induction hypothesis implies $\frac{q}{r_0} = \langle a_1, \dots, a_n \rangle$. Therefore,

$$\frac{p}{q} = a_0 + \frac{r_0}{q} = a_0 + \frac{1}{\frac{q}{r_0}} = a_0 + \frac{1}{\langle a_1, \dots, a_n \rangle} \overset{1.2.2}{=} \langle a_0, \dots, a_n \rangle.$$

For the first equality, just divide the equation $p = a_0 q + r_0$ by q. □

Example 1.2.4. We calculate two finite continued fractions.

(a) First we work with $\frac{355}{113}$ (do you recognize this?). The Euclidean algorithm gives

$$\begin{aligned} 355 &= \mathbf{3} \cdot 113 + 16 \\ 113 &= \mathbf{7} \cdot 16 + 1 \\ 16 &= \mathbf{16} \cdot 1 + 0 \end{aligned}$$

Hence, $\frac{355}{113} = \langle 3, 7, 16 \rangle$.

(b) Recall the Fibonacci sequence $f_0 = 0$, $f_1 = 1$, and $f_{n+1} = f_n + f_{n-1}$ for all $n \in \mathbb{N}$. Obviously, this sequence is strictly increasing for $n \geq 2$. For any $n \geq 2$ the Euclidean algorithm of two consecutive Fibonacci numbers reads

$$\begin{aligned} f_{n+1} &= \mathbf{1} \cdot f_n + f_{n-1} \\ f_n &= \mathbf{1} \cdot f_{n-1} + f_{n-2} \\ &\vdots \\ f_4 &= \mathbf{1} \cdot f_3 + f_2 \\ f_3 &= \mathbf{2} \cdot f_2 + 0 \end{aligned}$$

Therefore,

$$\frac{f_{n+1}}{f_n} = \langle \underbrace{1, \dots, 1}_{(n-2)\text{-times}}, 2 \rangle = \langle \underbrace{1, \dots, 1}_{(n-2)\text{-times}}, 1 + \frac{1}{1} \rangle \overset{1.2.2}{=} \langle \underbrace{1, \dots, 1}_{n\text{-times}} \rangle.$$

We see, that the representation of a rational number by a finite continued fraction is not unique. But the next lemma tells us, that the situation is still quite comfortable.

Lemma 1.2.5. *For every $\alpha \in \mathbb{Q}$ there are precisely two representations of α as a finite continued fraction. For $\alpha \in \mathbb{Z}$ these are $\langle \alpha \rangle$ and $\langle \alpha - 1, 1 \rangle$. For $\alpha \in \mathbb{Q} \setminus \mathbb{Z}$ these are of the form $\langle a_0, \dots, a_n \rangle$, $a_n \geq 2$, and $\langle a_0, \dots, a_n - 1, 1 \rangle$.*

Proof. As usual we write $\alpha = \frac{p}{q}$, $q \geq 1$, $\gcd(p, q) = 1$, and perform an induction on q. In the induction base we have $q = 1$, which is precisely the case when $\alpha \in \mathbb{Z}$. We have $\alpha = \langle a_0 \rangle$ if and only if $\alpha = a_0$. So assume $\alpha = \langle a_0, \dots, a_n \rangle$, with $n \geq 1$. Then $\alpha = a_0 + \frac{1}{\langle a_1, \dots, a_n \rangle}$, and $\langle a_1, \dots, a_n \rangle \overset{1.2.2}{\geq} a_1 \geq 1$. But $\frac{1}{\langle a_1, \dots, a_n \rangle} = \alpha - a_0$ is an integer. Hence $\langle a_1, \dots, a_n \rangle = 1$. Again by Lemma 1.2.2, this is precisely the case when $n = 1$ and $a_1 = 1$. It follows that

$\alpha = \langle a_0, 1\rangle = a_0 + \frac{1}{1}$, and therefore $a_0 = \alpha - 1$. This gives that $\alpha = \langle \alpha - 1, 1\rangle$ is the only representation of α as a finite continued fraction with more than one entry.
Our induction hypothesis is, that for fixed $q > 1$ the statement of the lemma is true for all rational numbers $\frac{p'}{q'}$, with $q' \in \{1, \dots, q-1\}$.
For the induction step, we take a rational number $\alpha = \frac{p}{q} = \langle a_0, \dots, a_n\rangle$ (with q from the induction hypothesis). Since $q > 1$, we know that α is not an integer, and hence $n \geq 1$. As in the proof of the induction base, we have

$$\alpha = \frac{p}{q} = a_0 + \underbrace{\frac{1}{\langle a_1, \dots, a_n\rangle}}_{\in(0,1)}$$

But this just means that $a_0 = \left\lfloor \frac{p}{q} \right\rfloor$ and $\frac{1}{\langle a_1, \dots, a_n\rangle} = \left\{\frac{p}{q}\right\}$. In particular, there is just one possible value for a_0, which is the same as a_0 *is uniquely determined.*
Moreover,

$$1 \leq a_1 < \langle a_1, \dots, a_n\rangle = \frac{1}{\langle 0, a_1, \dots, a_n\rangle} = \left(\frac{p}{q} - a_0\right)^{-1} = \frac{q}{p - qa_0}.$$

Hence, $\langle a_1, \dots, a_n\rangle = \frac{q}{u}$, for some $u \in \{1, \dots, q-1\}$. Now we can apply our induction hypothesis, and we can conclude that there precisely two finite continued fraction representations of $\frac{q}{u}$, namely $\langle a_1, \dots, a_n\rangle$, with $a_n \geq 2$, and $\langle a_1, \dots, a_n - 1, 1\rangle$. Since we already know that a_0 is uniquely determined, the lemma is proved. □

Remark 1.2.6. Given $a_0 \in \mathbb{Z}$ and $a_1, \dots, a_n \in \mathbb{N}$, we can calculate $p, q \in \mathbb{Z}$ with $\langle a_0, \dots, a_n\rangle = \frac{p}{q}$ by successively calculating

$$\langle a_0, \dots, a_n\rangle = \langle a_0, \dots, \underbrace{a_{n-1} + \frac{1}{a_n}}_{=p'/q'}\rangle = \langle a_0, \dots, \underbrace{a_{n-2} + \frac{q'}{p'}}_{=p''/q''}\rangle = \dots$$

This is, we can calculate p and q by going from right to left, which can become quite painful for large n. In the following proposition we will introduce an important recursive formula, which allows us to calculate p and q from left to right.

Proposition 1.2.7. *Let $a_0 \in \mathbb{Z}$ and $a_1, a_2, \dots$ be an infinite sequence of natural numbers. We define*

$$p_{-2} = 0,\ p_{-1} = 1, \quad \text{and} \quad p_k = a_k p_{k-1} + p_{k-2} \quad \forall\ k \in \mathbb{N}_0$$

$$q_{-2} = 1,\ q_{-1} = 0, \quad \text{and} \quad q_k = a_k q_{k-1} + q_{k-2} \quad \forall\ k \in \mathbb{N}_0$$

Then we have $\langle a_0, \dots, a_n, x\rangle = \frac{xp_n + p_{n-1}}{xq_n + q_{n-1}}$ for all integers $n \geq -1$ and all real numbers $x > 0$.

Proof. Induction again: For $n = -1$ we have $\langle a_0, \dots, a_n, x\rangle = \langle x\rangle = \frac{x\cdot 1 + 0}{x\cdot 0 + 1} = \frac{xp_n + p_{n-1}}{xq_n + q_{n-1}}$ for all $x \in \mathbb{R}$, which provides the induction base.

Now we assume that the equation holds for all real $x > 0$ for a fixed $n \geq -1$. Then we get for any real $x > 0$

$$\begin{aligned}\langle a_0, \ldots, a_{n+1}, x\rangle &= \langle a_0, \ldots, a_n, a_{n+1} + \frac{1}{x}\rangle \\ &\overset{\text{IH}}{=} \frac{(a_{n+1} + \frac{1}{x})p_n + p_{n-1}}{(a_{n+1} + \frac{1}{x})q_n + q_{n-1}} = \frac{x(a_{n+1}p_n + p_{n-1}) + p_n}{x(a_{n+1}q_n + q_{n-1}) + q_n} \\ &\overset{\text{Def}}{=} \frac{xp_{n+1} + p_n}{xq_{n+1} + q_n}.\end{aligned}$$

This proves the proposition. □

Corollary 1.2.8. *In the notation from Proposition 1.2.7, we have* $\langle a_0, \ldots, a_n\rangle = \frac{p_n}{q_n}$ *for all* $n \in \mathbb{N}_0$.

Proof. By Proposition 1.2.3 it follows

$$\langle a_0, \ldots, a_n\rangle = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}.$$

□

Example 1.2.9. The integers p_n and q_n are defined recursively, and hence *from left to right*. Which rational number is represented by $\langle 2, 1, 2, 1, 1, 4\rangle$? We just need to calculate p_5 and q_5. This is most convenient using the following table

k	a_k	p_k	q_k
-2	-	0	1
-1	-	1	0
0	2	2	1
1	1	3	1
2	2	8	3
3	1	11	4
4	1	19	7
5	4	87	32

It follows $\langle 2, 1, 2, 1, 1, 4\rangle = \frac{87}{32}$ (and $\langle 2, 1, 2, 1, 1\rangle = \frac{19}{7}$, and $\langle 2, 1, 2, 1\rangle = \frac{11}{4}$, ...).

Remark 1.2.10. The idea is, that $\frac{p_0}{q_0}$, $\frac{p_1}{q_1}$, $\frac{p_2}{q_2}$, ... approximate $\frac{p_n}{q_n} = \langle a_0, \ldots, a_n\rangle$ with an increasing accuracy (check this for the values in Example 1.2.9). Since we want to approximate real numbers and not only rational numbers we have to generalize our continued fractions before we can prove the vague statement above.

Exercises

Exercise 1.7. (a) Write $\frac{123}{73}$ as a continued fraction.

(b) Let $n \geq 2$ be an integer. Write the continued fraction $\langle 1, n-1, 1, 3, n\rangle$ as a rational number $\frac{p}{q}$, with integers p, q depending on n.

Exercise 1.8. Let $a_0 \in \mathbb{Z}$ and $a_1, a_2 \ldots \in \mathbb{N}$. Moreover, let p_k and q_k be defined as in Proposition 1.2.7. Prove that for every $n \in \mathbb{N}_0$ we have

$$\langle a_n, a_{n-1}, \ldots, a_1\rangle = \frac{q_n}{q_{n-1}} \quad \text{and} \quad \langle 0, a_n, a_{n-1}, \ldots, a_1\rangle = \frac{q_{n-1}}{q_n}.$$

1.3 Infinite Continued Fractions

Notation 1.3.1. In this section we will extensively use the notations from Proposition 1.2.7, which we recall here:

- $a_0 \in \mathbb{Z}$, and $a_1, a_2, \ldots$ is an infinite sequence of natural numbers.
- $p_{-2} = 0$, $p_{-1} = 1$, and $p_k = a_k p_{k-1} + p_{k-2}$ for all $k \in \mathbb{N}_0$.
- $q_{-2} = 1$, $q_{-1} = 0$, and $q_k = a_k q_{k-1} + q_{k-2}$ for all $k \in \mathbb{N}_0$.

Lemma 1.3.2. *We use Notation 1.3.1. Then we have*

(i) $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$ *for all integers* $n \geq -1$.

(ii) $1 = q_0 \leq q_1 < q_2 < q_3 < \ldots$, *which means that* $(q_n)_{n\in\mathbb{N}}$ *is strictly increasing.*

(iii) $\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_{n+1}q_n}$ *for all* $n \in \mathbb{N}_0$.

(iv) $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots$, *which means that* $(\frac{p_{2n}}{q_{2n}})_{n\in\mathbb{N}_0}$ *is strictly increasing.*

(v) $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \ldots$, *which means that* $(\frac{p_{2n+1}}{q_{2n+1}})_{n\in\mathbb{N}_0}$ *is strictly decreasing.*

Proof. None of these statements requires any deep thoughts.

(i) For $n = -1$ we have $p_{-1}q_{-2} - q_{-1}p_{-2} = 1\cdot 1 - 0\cdot 0 = (-1)^{-1-1}$, which gives the induction base. Now assume that the equation is correct for fixed but arbitrary $n \geq -1$. Then

$$\begin{aligned} p_{n+1}q_n - q_{n+1}p_n &= (a_{n+1}p_n + p_{n-1})q_n - (a_{n+1}q_n + q_{n-1})p_n \\ &= p_{n-1}q_n - q_{n-1}p_n = (-1)\cdot(p_n q_{n-1} - q_n p_{n-1}) \\ &\overset{\text{IH}}{=} (-1)\cdot(-1)^{n-1} = (-1)^{(n+1)-1}. \end{aligned}$$

This proves the first statement of the lemma.

(ii) This follows from

$$1 = a_0 \cdot \underbrace{q_{-1}}_{=0} + \underbrace{q_{-2}}_{=1} = q_0 \leq a_1 \cdot \underbrace{q_0}_{=1} + \underbrace{q_{-1}}_{=0} = q_1 < \underbrace{a_2 q_1}_{\geq q_1} + \underbrace{q_0}_{\geq 1} = q_2 < \underbrace{a_3 q_2}_{\geq q_2} + \underbrace{q_1}_{\geq 1} = q_3 < \ldots$$

We will not not give the formal induction, since the statement should be clear enough now.

(iii) For any $n \in \mathbb{N}_0$ we have

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{p_{n+1}q_n - q_{n+1}p_n}{q_{n+1}q_n} \overset{(i)}{=} \frac{(-1)^n}{q_{n+1}q_n}.$$

(iv) Let $n \in \mathbb{N}$ be arbitrary. Then we have

$$\begin{aligned} \frac{p_{2n}}{q_{2n}} - \frac{p_{2n-2}}{q_{2n-2}} &= \left(\frac{p_{2n}}{q_{2n}} - \frac{p_{2n-1}}{q_{2n-1}}\right) + \left(\frac{p_{2n-1}}{q_{2n-1}} - \frac{p_{2n-2}}{q_{2n-2}}\right) \\ &\overset{(iii)}{=} \frac{(-1)^{2n-1}}{q_{2n}q_{2n-1}} + \frac{(-1)^{2n-2}}{q_{2n-1}q_{2n-2}} \\ &= \frac{1}{q_{2n-1}q_{2n-2}} - \frac{1}{q_{2n}q_{2n-1}} \overset{(ii)}{>} 0. \end{aligned}$$

This proves part (iv) and part (v) follows from exactly the same argument.

□

Proposition 1.3.3. *Let $a_0 \in \mathbb{Z}$ and $a_1, a_2, \ldots \in \mathbb{N}$ be an infinite sequence. Then the limit $\lim_{n\to\infty}\langle a_0, \ldots, a_n\rangle$ exists and is irrational.*

Proof. As always we will use the notation from 1.3.1. Then $\langle a_0, \ldots, a_n\rangle = \frac{p_n}{q_n}$ for all $n \in \mathbb{N}_0$ by Corollary 1.2.8. Hence, we have to prove that $\lim_{n\to\infty} \frac{p_n}{q_n}$ exists and is irrational.
We already know from Lemma 1.3.2 that the sequence $(\frac{p_{2n}}{q_{2n}})_{n\in\mathbb{N}_0}$ is strictly increasing, and the sequence $(\frac{p_{2n+1}}{q_{2n+1}})_{n\in\mathbb{N}_0}$ is strictly decreasing. Moreover, we have for all $n \in \mathbb{N}$

$$\frac{p_{2n}}{q_{2n}} \overset{1.3.2}{=} \frac{p_{2n-1}}{q_{2n-1}} - \frac{1}{q_{2n}q_{2n-1}} < \frac{p_{2n-1}}{q_{2n-1}} \leq \frac{p_1}{q_1} \quad \text{and} \quad \frac{p_{2n+1}}{q_{2n+1}} \overset{1.3.2}{=} \frac{p_{2n}}{q_{2n}} + \frac{1}{q_{2n+1}q_{2n}} > \frac{p_{2n}}{q_{2n}} \geq \frac{p_0}{q_0}.$$

So, the sequence $(\frac{p_{2n}}{q_{2n}})_{n\in\mathbb{N}_0}$ is strictly increasing and bounded from above by $\frac{p_1}{q_1}$. Hence, $E = \lim_{n\to\infty} \frac{p_{2n}}{q_{2n}}$ exists, and the same argument yields that $N = \lim_{n\to\infty} \frac{p_{2n+1}}{q_{2n+1}}$ exists.
We are left to prove $N = E$. But this follows again from Lemma 1.3.2, since

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{1}{q_{2n+1}q_{2n}} \overset{n\to\infty}{\longrightarrow} 0.$$

This proves the existence of $\lim_{n\to\infty} \frac{p_n}{q_n} = \lim_{n\to\infty}\langle a_0, \ldots, a_n\rangle$. Since the sequence with even indices is strictly increasing, and the sequence with odd indices is strictly decreasing, we have

$$\frac{p_{2k+1}}{q_{2k+1}} > \lim_{n\to\infty} \frac{p_n}{q_n} > \frac{p_{2k}}{q_{2k}} \quad \forall\, k \in \mathbb{N}_0. \tag{1.5}$$

In particular,

$$\left|\lim_{n\to\infty} \frac{p_n}{q_n} - \frac{p_k}{q_k}\right| < \left|\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right| \overset{1.3.2}{=} \frac{1}{q_{k+1}q_k} \quad \forall\, k \in \mathbb{N}_0, \tag{1.6}$$

which implies

$$\left|q_k \lim_{n\to\infty} \frac{p_n}{q_n} - p_k\right| < \frac{1}{q_{k+1}} \overset{k\to\infty}{\longrightarrow} 0.$$

By Corollary 1.1.7, it follows that $\lim_{n\to\infty} \frac{p_n}{q_n}$ must be irrational (it can be approximated too good, to be a rational number). □

Definition 1.3.4. For $a_0 \in \mathbb{Z}$ and an infinite sequence $a_1, a_2, \ldots \in \mathbb{N}$, we set $\langle a_0, a_1, \ldots\rangle = \lim_{n\to\infty}\langle a_0, \ldots, a_n\rangle$ and call this an *infinite continued fraction.*

As we have seen above, for any sequence $\langle a_0, a_1, \ldots\rangle$ exists and is a real irrational number.

Example 1.3.5. We already have calculated an explicit example in 1.2.4:

$$\langle 1, 1, 1, \ldots\rangle = \lim_{n\to\infty} \langle \underbrace{1, \ldots, 1}_{n \text{ times}}\rangle = \lim_{n\to\infty} \frac{f_{n+1}}{f_n} = \frac{\sqrt{5}+1}{2}.$$

Here, $f_0, f_1, f_2, \ldots$ are the Fibonacci numbers. The last equation is a standard property of Fibonacci numbers. The value $\frac{\sqrt{5}+1}{2}$ is called the *golden ratio.*

We already know that every rational number can be represented (in precisely two ways) as a finite continued fraction. We had two representatives, since we could manipulate the last entry of the finite continued fraction. In an infinite continued fraction, there is no last entry, which is essentially the argument for the uniqueness in the following proposition.

Proposition 1.3.6. *For all $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, there are unique integers $a_0, a_1, \ldots$, with $a_1, a_2, \ldots \geq 1$, such that $\alpha = \langle a_0, a_1, \ldots\rangle$.*

Proof. As in the rational case, the proof is constructive. Actually, a kind of Euclidean algorithm for non-integers is hidden in this proof. Define

$$\alpha_0 = \alpha, \quad \text{and} \quad \alpha_n = \frac{1}{\{\alpha_{n-1}\}} = \frac{1}{\alpha_{n-1} - \lfloor \alpha_{n-1}\rfloor} \quad \forall\, n \in \mathbb{N}.$$

Since $\alpha = \alpha_0$ is irrational, we have $\{\alpha_0\} = \alpha_0 - \lfloor \alpha_0\rfloor \in (0,1)$, and $\alpha_1 > 1$ is again irrational. Inductively, it follows that $\alpha_n > 1$ is irrational for all $n \in \mathbb{N}$. In particular, every α_n is well-defined. Note, that $\alpha_n = \lfloor \alpha_n\rfloor + \{\alpha_n\} = \lfloor \alpha_n\rfloor + \frac{1}{\alpha_{n+1}}$ for all $n \in \mathbb{N}_0$. Using this equation, we have

$$\begin{aligned}\alpha = \alpha_0 &= \langle \lfloor \alpha_0\rfloor + \frac{1}{\alpha_1}\rangle \overset{1.2.2}{=} \langle \lfloor \alpha_0\rfloor, \alpha_1\rangle = \langle \lfloor \alpha_0\rfloor, \lfloor \alpha_1\rfloor + \frac{1}{\alpha_2}\rangle \overset{1.2.2}{=} \langle \lfloor \alpha_0\rfloor, \lfloor \alpha_1\rfloor, \alpha_2\rangle \\ &= \ldots = \langle \lfloor \alpha_0\rfloor, \lfloor \alpha_1\rfloor, \lfloor \alpha_2\rfloor, \ldots, \lfloor \alpha_n\rfloor, \alpha_{n+1}\rangle \quad \forall\, n \in \mathbb{N}. \end{aligned} \tag{1.7}$$

Now you should have an idea how the infinite continued fraction for α looks like. We set $\lfloor \alpha_n\rfloor = a_n$ for all $n \in \mathbb{N}_0$. Since $\alpha_n > 1$ for all $n \in \mathbb{N}$, we know that $a_n \in \mathbb{N}$ for all $n \in \mathbb{N}$. With p_n and q_n as usual (see 1.3.1), we get

$$\alpha_{n+1}q_n + q_{n-1} > \lfloor \alpha_{n+1}\rfloor\, q_n + q_{n-1} = a_{n+1}q_n + q_{n-1} = q_{n+1} \quad \forall\, n \in \mathbb{N}_0. \tag{1.8}$$

It follows:

$$\begin{aligned}\left|\alpha - \frac{p_n}{q_n}\right| &\overset{(1.7)}{=} \left|\langle a_0, a_1, \ldots, a_n, \alpha_{n+1}\rangle - \frac{p_n}{q_n}\right| \overset{1.2.7}{=} \left|\frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n}\right| \\ &= \left|\frac{(\alpha_{n+1}p_n + p_{n-1})q_n - (\alpha_{n+1}q_n + q_{n-1})p_n}{(\alpha_{n+1}q_n + q_{n-1})q_n}\right| = \left|\frac{p_{n-1}q_n - q_{n-1}p_n}{(\alpha_{n+1}q_n + q_{n-1})q_n}\right| \\ &\overset{1.3.2}{=} \frac{1}{(\alpha_{n+1}q_n + q_{n-1})q_n} \overset{(1.8)}{<} \frac{1}{q_{n+1}q_n}. \end{aligned} \tag{1.9}$$

Since $\frac{1}{q_{n+1}q_n}$ tends to zero as n tends to infinity, we finally achieve

$$\alpha = \lim_{n\to\infty} \frac{p_n}{q_n} = \lim_{n\to\infty} \langle a_0, \ldots, a_n\rangle = \langle a_0, a_1, \ldots\rangle.$$

So in particular every real irrational α can be written as an infinite continued fraction. It remains to prove the uniqueness of the a_n's. Therefore, let $\alpha = \langle b_0, b_1, \ldots\rangle$ for some integers $b_0, b_1, \ldots$. Then $\alpha = b_0 + \frac{1}{\langle b_1, \ldots\rangle}$, and $\frac{1}{\langle b_1, \ldots\rangle} \in (0,1)$. It follows, $b_0 = \lfloor \alpha\rfloor = a_0$. Moreover, $\alpha_1 = \langle b_1, \ldots\rangle$, and as before we see that $b_1 = \lfloor \alpha_1\rfloor = a_1$. It follows inductively that $b_n = a_n$ for all $n \in \mathbb{N}_0$. Hence, there is just one representation of α as an infinite continued fraction. □

Remark 1.3.7. The values $\alpha_0, \alpha_1, \ldots$ from the proof above will be used throughout this chapter. Note that the construction ensures, that $\alpha_k = \langle a_k, a_{k+1}, a_{k+2}, \ldots\rangle$ (see (1.7)). This is in harmony with the fundamental properties 1.2.2, since we have

$$\langle a_0, a_1, \ldots, a_{k-1}, \alpha_k\rangle = \alpha = \langle a_0, \ldots, a_{k-1}, \langle a_k, a_{k+1}, \ldots\rangle\rangle.$$

Example 1.3.8. As mentioned in the proof, we now have a perfectly explicit method to construct the entries of an infinite continued fraction.

(a) Let us write $\sqrt{2}$ as an infinite continued fraction. We set $\alpha_0 = \sqrt{2}$, and $a_0 = \lfloor \sqrt{2} \rfloor = 1$. Then $\alpha_1 = \frac{1}{\sqrt{2}-1}$ and

$$a_1 = \left\lfloor \frac{1}{\sqrt{2}-1} \right\rfloor = \left\lfloor \frac{\sqrt{2}+1}{(\sqrt{2}-1)(\sqrt{2}+1)} \right\rfloor = \lfloor \sqrt{2}+1 \rfloor = 2.$$

Next, we have $\alpha_2 = \frac{1}{\alpha_1 - \lfloor \alpha_1 \rfloor} = \frac{1}{\sqrt{2}+1-2} = \alpha_1$ and hence $a_2 = a_1 = 2$.

Since $\alpha_1 = \alpha_2$, it is also $\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{1}{\alpha_1 - a_1} = \alpha_2$ (and in particular $a_3 = a_2 = a_1$). This is, we are in a loop and have $a_n = a_1 = 2$ for all $n \in \mathbb{N}$. Hence

$$\sqrt{2} = \langle 1, 2, 2, 2, 2, 2, \ldots \rangle.$$

(b) Without proof we mention that the infinite continued fraction for e looks like

$$\langle 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, 1, \ldots \rangle$$

For a proof of this we refer to Sections 2.10 and 2.11 of [2].

(c) Of course "most" continued fractions do not follow such a nice pattern. We will calculate the first few entries of the continued fraction for π.

$$\begin{aligned}
a_0 &= \lfloor \pi \rfloor = 3 \\
a_1 &= \left\lfloor \frac{1}{\pi - 3} \right\rfloor = 7 \\
a_2 &= \left\lfloor \frac{1}{\frac{1}{\pi-3} - 7} \right\rfloor = \left\lfloor \frac{\pi - 3}{-7\pi + 22} \right\rfloor = 15 \\
a_3 &= \left\lfloor \frac{1}{\frac{\pi-3}{-7\pi+22} - 15} \right\rfloor = \left\lfloor \frac{-7\pi + 22}{106\pi - 333} \right\rfloor = 1
\end{aligned}$$

Hence, $\pi = \langle 3, 7, 15, 1, \ldots \rangle$.

Definition 1.3.9. In the usual notation, for any $n \in \mathbb{N}_0$ we call $\frac{p_n}{q_n} \overset{1.2.8}{=} \langle a_0, \ldots, a_n \rangle$ the *n-th convergent* of the infinite continued fraction $\langle a_0, a_1, \ldots \rangle$.

Remark 1.3.10. We know that $p_n q_{n-1} - q_n p_{n-1} = \pm 1$. Hence, by Bézout's lemma, we have $\gcd(p_n, q_n) = 1$ for all $n \in \mathbb{N}_0$. We have seen in Proposition 1.3.3 that

$$\lim_{n \to \infty} \left| \langle a_0, a_1, \ldots \rangle - \frac{p_n}{q_n} \right| = 0.$$

Hence, the rational numbers $\frac{p_n}{q_n}$ are indeed approximations of $\alpha = \langle a_0, a_1, \ldots \rangle$ with increasing accuracy.

Example 1.3.11. The first convergents of $\sqrt{2} = \langle 1, 2, 2, 2, 2, \ldots \rangle$ are

k	a_k	p_k	q_k	$\frac{p_k}{q_k}$
-2	–	0	1	–
-1	–	1	0	–
0	1	1	1	1
1	2	3	2	$\frac{3}{2}$
2	2	7	5	$\frac{7}{5}$
3	2	17	12	$\frac{17}{12}$
4	2	41	29	$\frac{41}{29}$
5	2	99	70	$\frac{99}{70}$
6	2	239	169	$\frac{239}{169}$

One application of this, was the size of an A4 paper. In order that a A4 paper looks like a small A3 paper, such that the width of the A3 paper is the height of the A4 paper, the side length of an A4 paper should have the ratio $\sqrt{2}$. But of course, one would like to be able to measure everything in full millimetres. Hence, the side-ratio should be approximately $\sqrt{2}$. In fact it is $\frac{297}{210} = \frac{99}{70}$, the fifth convergent.
The same argument yields, that the side-ratio of any A paper should be approximately $\sqrt{2}$. In addition, the area of an A0 paper should be approximately $1m^2$. Try to figure out the actual side-ratio of an A0 paper!

Next we will show, that the convergents of α are actually the *best possible* approximations of α. Therefore, the following theorem is sometimes called the *law of best approximation.*

Theorem 1.3.12. *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be arbitrary, and let $\alpha = \langle a_0, a_1, a_2, \ldots \rangle$ and p_n, q_n be as in Notation 1.3.1. Then*

(i) $|q_n\alpha - p_n| > |q_{n+1}\alpha - p_{n+1}|$ *for all* $n \in \mathbb{N}_0$.

(ii) For fixed $n \in \mathbb{N}$ *let* $p \in \mathbb{Z}$, $q \in \mathbb{N}$, *with* $q \leq q_n$ *and* $(p, q) \neq (p_n, q_n)$. *Then* $|q\alpha - p| \geq |q_{n-1}\alpha - p_{n-1}|$.

Remark 1.3.13. Note, that Theorem 1.3.12 implies that $|\alpha - \frac{p}{q}| > |\alpha - \frac{p_n}{q_n}|$, whenever $q \leq q_n$ and $\frac{p}{q} \neq \frac{p_n}{q_n}$. This means that $\frac{p_n}{q_n}$ is the best approximation for α among all rational numbers with positive denominator $\leq q_n$.

Proof of Theorem 1.3.12. The first statement is quite easy to prove. The proof of the second statement goes back to Lagrange.

(i) Let $n \in \mathbb{N}_0$ be arbitrary. We use the notation from the proof of Proposition 1.3.6. This is $\alpha_0 = \alpha$, and $\alpha_k = \frac{1}{\{\alpha_{k-1}\}}$ for all $k \in \mathbb{N}$. As seen in the proof of Proposition 1.3.6, we have

$$1 < \alpha_{n+2} \quad \text{and} \quad \alpha_{n+1} = a_{n+1} + \frac{1}{\alpha_{n+2}} < a_{n+1} + 1. \tag{1.10}$$

This implies

$$\begin{aligned} |q_{n+1}\alpha - p_{n+1}| &\overset{(1.9)}{=} \frac{1}{\alpha_{n+2}q_{n+1} + q_n} \overset{(1.10)}{<} \frac{1}{q_{n+1} + q_n} \\ &= \frac{1}{a_{n+1}q_n + q_{n-1} + q_n} = \frac{1}{(a_{n+1}+1)q_n + q_{n-1}} \\ &\overset{(1.10)}{<} \frac{1}{\alpha_{n+1}q_n + q_{n-1}} \overset{(1.9)}{=} |q_n\alpha - p_n|, \end{aligned}$$

which proves part (i) of the theorem.

(ii) Let p, q, and n be as in the statement. We again apply the fundamental property $p_nq_{n-1}-q_np_{n-1}=\pm 1$. The left hand side is the determinant of the matrix $\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$. In particular, this determinant is invertible in $\mathbb{Z}$, and hence the matrix is in $GL_2(\mathbb{Z})$. So, there are $k, \ell \in \mathbb{Z}$ such that

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \cdot \begin{pmatrix} k \\ l \end{pmatrix} = \begin{pmatrix} p \\ q \end{pmatrix}. \tag{1.11}$$

We distinguish between several cases. Note that $q \in \mathbb{N}$, and hence k and ℓ cannot both be equal to zero.

1. case: $\ell = 0$**,** $k \neq 0$

Then $kp_n = p$ and $kq_n = q$. But since $q \leq q_n$, it follows $k = 1$, which implies $(p, q) = (p_n, q_n)$. This contradicts our assumption, and hence this case is not possible.

2. case: $k = 0$**,** $\ell \neq 0$

Then $\ell p_{n-1} = p$ and $\ell q_{n-1} = q$. This implies the claim, since

$$|q\alpha - p| = |\ell| \cdot |q_{n-1}\alpha - p_{n-1}| \geq |q_{n-1}\alpha - p_{n-1}|.$$

3. case: $k\ell \neq 0$

We already know that $\frac{p_n}{q_n} > \alpha$ if n is odd and $\frac{p_n}{q_n} < \alpha$ if n is even. Since q_n and q_{n-1} are both positive (and precisely one of n and $n-1$ is even), it follows that $q_n\alpha - p_n$ and $q_{n-1}\alpha - p_{n-1}$ have opposite signs (one is positive, the other is negative). Moreover, by (1.11) we have $kq_n + \ell q_{n-1} = q$, and $|kq_n| + |\ell q_{n-1}| \overset{k\neq 0}{>} q_n \geq q$. Therefore, k and ℓ must be of opposite sign, too. Multiplying the pairs (k, ℓ) and $(q_n\alpha - p_n, q_{n-1}\alpha - p_{n-1})$ of opposite signs, yields that $k \cdot (q_n\alpha - p_n)$ and $\ell \cdot (q_{n-1}\alpha - p_{n-1})$ have the same sign. (If you doubt this conclusion: check all four possible combinations!).

Since these two terms have the same sign, we get

$$|k \cdot (q_n\alpha - p_n)| + |\ell \cdot (q_{n-1}\alpha - p_{n-1})| = |k \cdot (q_n\alpha - p_n) + \ell \cdot (q_{n-1}\alpha - p_{n-1})| = |q\alpha - p|.$$

The values $|k \cdot (q_n\alpha - p_n)|$ and $|\ell \cdot (q_{n-1}\alpha - p_{n-1})|$ are both positive, and hence

$$|q\alpha - p| > |\ell \cdot (q_{n-1}\alpha - p_{n-1})| \overset{\ell\neq 0}{\geq} |q_{n-1}\alpha - p_{n-1}|,$$

which proves statement (ii).

□

Corollary 1.3.14. *With $\alpha = \langle a_0, a_1, \ldots \rangle$ and p_n, q_n as usual, we have*

$$\liminf_{(p,q)\in\mathbb{Z}\times\mathbb{N}} q^2 \cdot \left|\alpha - \frac{p}{q}\right| = \liminf_{n\to\infty} q_n^2 \cdot \left|\alpha - \frac{p_n}{q_n}\right|.$$

Proof. Let us first note some simple facts, which will be used later. By Dirichlet 1.1.9 we have $\liminf_{(p,q)\in\mathbb{Z}\times\mathbb{N}} q^2 \cdot \left|\alpha - \frac{p}{q}\right| \leq 1$. Moreover, for any fixed $q \in \mathbb{N}$ it is $\liminf_{p\in\mathbb{Z}} q^2 \cdot \left|\alpha - \frac{p}{q}\right| = \infty$. Hence, in any sequence of rational numbers $\frac{p}{q}$ such that $q^2 \cdot \left|\alpha - \frac{p}{q}\right|$ converges, the denominators q tend to infinity.
Obviously, we have $\liminf_{(p,q)\in\mathbb{Z}\times\mathbb{N}} q^2 \cdot \left|\alpha - \frac{p}{q}\right| \leq \liminf_{n\to\infty} q_n^2 \cdot \left|\alpha - \frac{p_n}{q_n}\right|$. In order to prove equality, let $(p, q) \in \mathbb{Z} \times \mathbb{N}$ be arbitrary. By our introductory remarks, it is enough to prove that there is some convergent $\frac{p_n}{q_n}$ such that $q^2 \cdot \left|\alpha - \frac{p}{q}\right| \geq q_n^2 \cdot \left|\alpha - \frac{p_n}{q_n}\right|$.
There is an $n \in \mathbb{N}$ such that $q_{n-1} \leq q < q_n$. For this n, we have

$$\begin{aligned}
& q \cdot \left|\alpha - \frac{p}{q}\right| \overset{1.3.12}{\geq} q_{n-1} \cdot \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| \\
\implies \quad & q^2 \cdot \left|\alpha - \frac{p}{q}\right| \geq q \cdot q_{n-1} \cdot \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| \geq q_{n-1}^2 \cdot \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| \\
\implies \quad & \liminf_{n\to\infty} q_n^2 \cdot \left|\alpha - \frac{p_n}{q_n}\right| \leq \liminf_{(p,q)\in\mathbb{Z}\times\mathbb{N}} q^2 \cdot \left|\alpha - \frac{p}{q}\right|,
\end{aligned}$$

proving the claim. □

Remark 1.3.15. For $\alpha = \langle a_0, a_1, \ldots, \rangle = \lim_{n\to\infty} \frac{p_n}{q_n}$, we have $q_1 < q_2 < q_3 < \ldots$, and from (1.6) we know

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} = \frac{1}{q_n^2 \cdot \frac{q_{n+1}}{q_n}} \quad \forall\, n \in \mathbb{N}.$$

Since the convergents $\frac{p_n}{q_n}$ are the best approximations of α, it follows that α can be approximated particularly well, if the q_n's increase very fast, and particularly bad if the q_n's increase very slow. We have $q_{n+1} = a_{n+1}q_n + q_{n-1}$, hence the a_n's control how fast the q_n's increase. In particular, the golden ratio $\langle 1, 1, 1, \ldots \rangle \overset{1.3.5}{=} \frac{1+\sqrt{5}}{2}$ should be the *worst approximable* irrational number. We will make this precise in a moment. First, we improve the constant 1 in Dirichlet's approximation result (Corollary 1.1.9).

Lemma 1.3.16. *Let α and β be positive real numbers with $\alpha > \beta$. In the usual notation, we have*

$$\langle a_0, \ldots, a_n, \alpha \rangle > \langle a_0, \ldots, a_n, \beta \rangle \quad \iff \quad n \text{ is odd.}$$

Proof. This is a simple calculation:

$$\begin{aligned}
& \langle a_0, \ldots, a_n, \alpha \rangle > \langle a_0, \ldots, a_n, \beta \rangle \\
\overset{1.2.7}{\iff} \quad & \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}} > \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}} \\
\iff \quad & (\beta q_n + q_{n-1})(\alpha p_n + p_{n-1}) > (\alpha q_n + q_{n-1})(\beta p_n + p_{n-1}) \\
\iff \quad & (p_n q_{n-1} - q_n p_{n-1})\alpha > (p_n q_{n-1} - q_n p_{n-1})\beta \\
\overset{1.3.2}{\iff} \quad & (-1)^{n-1}\alpha > (-1)^{n-1}\beta
\end{aligned}$$

This proves the claim, since $\alpha > \beta$ by hypothesis. □

Theorem 1.3.17. *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be arbitrary. There are infinitely many rational numbers $\frac{p}{q}$, $q \geq 1$, such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}. \tag{1.12}$$

Proof. We again use $\alpha = \langle a_0, a_1, \ldots, a_n, \alpha_{n+1}\rangle$ for every $n \in \mathbb{N}_0$, where $\alpha_0 = 0$ and $\alpha_k = \frac{1}{\{\alpha_{k-1}\}}$ for all $k \in \mathbb{N}$. Recall from Proposition 1.3.6, that $a_k = \lfloor \alpha_k \rfloor < \alpha_k$ for all $k \in \mathbb{N}_0$. Since the convergents of α are the best approximations of α, we can restrict our attention to these rational numbers. We have

$$\left|\alpha - \frac{p_n}{q_n}\right| \overset{(1.9)}{=} \frac{1}{(\alpha_{n+1}q_n + q_{n-1})q_n} = \frac{1}{q_n^2 \cdot \frac{\alpha_{n+1}q_n + q_{n-1}}{q_n}} \quad \forall\, n \in \mathbb{N}.$$

Hence, in order to prove the theorem, we have to show that

$$\frac{\alpha_{n+1}q_n + q_{n-1}}{q_n} = \alpha_{n+1} + \frac{q_{n-1}}{q_n} > \sqrt{5} \quad \text{for infinitely many } n \in \mathbb{N}. \tag{1.13}$$

There are some smart arguments for this, but we will prove this straight-forward, chasing through several natural cases.

1. case: $a_n \geq 3$ for infinitely many $n \in \mathbb{N}$

Then for any $n \in \mathbb{N}$ such that $a_{n+1} \geq 3$ (there are infinitely many of those), we have

$$\alpha_{n+1} + \frac{q_{n-1}}{q_n} \geq 3 + \frac{q_{n-1}}{q_n} > 3 > \sqrt{5}.$$

This proves (1.13).

2. case: $a_n \geq 3$ only for finitely many $n \in \mathbb{N}$, but $a_n \geq 2$ for infinitely many $n \in \mathbb{N}$

For any $n \in \mathbb{N}$ such that $a_{n+1} = 2$ and $a_n \leq 2$ (there are infinitely many of those), we have $a_n + \frac{q_{n-2}}{q_{n-1}} < 2 + 1 = 3$ and hence

$$\alpha_{n+1} + \frac{q_{n-1}}{q_n} > a_{n+1} + \frac{q_{n-1}}{a_n q_{n-1} + q_{n-2}} = 2 + \frac{1}{a_n + \frac{q_{n-2}}{q_{n-1}}} > 2 + \frac{1}{3} > \sqrt{5}.$$

This proves (1.13).

3. case: $a_n \geq 2$ only for finitely many $n \in \mathbb{N}$

In this case, there is a $k \in \mathbb{N}_0$ such that

$$\alpha = \langle a_0, a_1, \ldots, a_k, 1, 1, 1, 1, 1, \ldots\rangle.$$

This is, k is at least the largest index, such that $a_k \geq 2$. In particular,

$$\alpha_n \overset{1.3.7}{=} \langle 1, 1, \ldots\rangle \overset{1.3.5}{=} \frac{1+\sqrt{5}}{2} \quad \forall n > k.$$

We use the statement of Exercise 1.8, to conclude

$$\alpha_{k+N+1} + \frac{q_{k+N-1}}{q_{k+N}} = \frac{1+\sqrt{5}}{2} + \langle 0, \underbrace{1,1,\ldots,1}_{N\text{-times}}, a_k, a_{k-1}, \ldots, a_1\rangle \quad \forall\, N \in \mathbb{N}. \tag{1.14}$$

The rational number $\langle a_k, \ldots, a_1\rangle$ is either greater or smaller than the golden ratio $\langle 1,1,\ldots\rangle = \frac{1+\sqrt{5}}{2}$. Hence, by Lemma 1.3.16, either for all odd N or for all even N, we have

$$\begin{aligned}
&\langle 0, \underbrace{1,1,\ldots,1}_{N\text{-times}}, a_k, a_{k-1}, \ldots, a_1\rangle = \langle 0, \underbrace{1,1,\ldots,1}_{N\text{-times}}, \langle a_k, a_{k-1}, \ldots, a_1\rangle\rangle \\
>&\langle 0, \underbrace{1,1,\ldots,1}_{N\text{-times}}, \langle 1,1,\ldots\rangle\rangle = \langle 0,1,1,1,\ldots\rangle \\
=&\frac{1}{\langle 1,1,1,\ldots\rangle} \overset{1.3.5}{=} \frac{2}{1+\sqrt{5}}.
\end{aligned} \tag{1.15}$$

Combining (1.14) and (1.15) yields that either for every odd N or for every even N (so in particular for infinitely many integers N) we have

$$\begin{aligned}
\alpha_{k+N+1} + \frac{q_{k+N-1}}{q_{k+N}} &\overset{(1.14)}{=} \frac{1+\sqrt{5}}{2} + \langle 0, \underbrace{1,1,\ldots,1}_{N\text{-times}}, a_k, a_{k-1}, \ldots, a_1\rangle \\
&\overset{(1.15)}{>} \frac{1+\sqrt{5}}{2} + \frac{2}{\sqrt{5}+1} = \frac{1+\sqrt{5}}{2} + \frac{-1+\sqrt{5}}{2} = \sqrt{5}.
\end{aligned}$$

This proves (1.13) also in this last case, which concludes the proof of the theorem. □

Remark 1.3.18. The proof of Theorem 1.3.17 tells us, that if there are only finitely many rational numbers $\frac{p}{q}$ such that $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\frac{7}{3}\cdot q^2}$, then α is of the form

$$\langle a_0, \ldots, a_k, 1,1,1\ldots\rangle = \langle a_0, \ldots, a_k, \frac{1+\sqrt{5}}{2}\rangle \in \mathbb{Q}(\sqrt{5}).$$

With some more care one can prove that one may replace $\frac{7}{3}$ by $\sqrt{8}$ in this statement. Moreover, the constant $\sqrt{5}$ in Theorem 1.3.17 is best possible: For $\alpha = \langle 1,1,\ldots\rangle$ Equation (1.14) implies that

$$\alpha_n + \frac{q_{n-2}}{q_{n-1}} \longrightarrow \frac{1+\sqrt{5}}{2} + \frac{1}{\langle 1,\ldots\rangle} = \sqrt{5}.$$

In particular, for any $\varepsilon > 0$ there are only finitely many rational numbers $\frac{p}{q}$, with $\left|\alpha - \frac{p}{q}\right| < \frac{1}{(\sqrt{5}+\varepsilon)q^2}$.

Definition 1.3.19. A real number $\alpha \in \mathbb{R}$ is called *badly approximable* if

$$\liminf_{\substack{(p,q)\in\mathbb{Z}\times\mathbb{N} \\ \gcd(p,q)=1}} q^2 \cdot \left|\alpha - \frac{p}{q}\right| > 0.$$

Remark 1.3.20. By Liouville's Theorem 1.1.12 for all $\alpha \in \overline{\mathbb{Q}}$ of degree ≤ 2, there is a constant $c > 0$ such that $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{\deg \alpha}}$, whenever $\frac{p}{q} \neq \alpha$. This shows that every $\alpha \in \overline{\mathbb{Q}}$ of degree ≤ 2 is badly approximable. The condition $\gcd(p,q) = 1$ is necessary, solely to exclude that $\alpha = \frac{p}{q}$ for infinitely many admissible pairs (p,q).

Proposition 1.3.21. *Let $\alpha = \langle a_0, a_1, \ldots \rangle$ be an irrational number. Then α is badly approximable if and only if there is a constant C such that $a_n < C$ for all $n \in \mathbb{N}_0$.*

Proof. We skip the proof. □

Exercises

Exercise 1.9. Let $\frac{p_n}{q_n}$ be the n-th convergent of $\sqrt{2}$. Prove that $\left|\sqrt{2}-1\right|^{n+1} = \left|q_n\sqrt{2} - p_n\right|$.

Exercise 1.10. Write $\sqrt{7}$ as an infinite continued fraction.

Exercise 1.11. We study the irrational number $\alpha = \langle a_0, a_1, a_2, \ldots \rangle$, with $a_n = 2^{n!}$ for all $n \in \mathbb{N}_0$. As usual $\frac{p_n}{q_n}$ is the n-th convergent of α. The aim is to prove that α is transcendental.

(a) Prove that for all $n \in \mathbb{N}_0$ we have $\frac{2^{(n+1)!}}{(2^{n!}+1)^{n-1}} \geq q_n$.

Hint: Check that the statement is correct for $n \in \{0, 1, 2\}$ and then proceed by induction. Note that $q_n \leq (a_n + 1)q_{n-1}$.

(b) Prove that for all $n \in \mathbb{N}$ we have $q_{n-1}^{n-1} < q_n$.

Hint: This is again an induction, and the inequality $q_n \leq (a_n + 1)q_{n-1}$ is still valid.

(c) Prove that α is transcendental.

Hint: The convergents should be very good approximations...

Hint: You may use (a) and (b) , whether you solved them or not.

Exercise 1.12. Let $\alpha \in \mathbb{R}$ be arbitrary and $\frac{p}{q} \in \mathbb{Q}$, with $q \in \mathbb{N}$.

(a) Let $\frac{P}{Q} \in \mathbb{Q}$ be another rational number with $Q \in \mathbb{N}$ and $\frac{P}{Q} \neq \frac{p}{q}$. Prove that $\frac{1}{qQ} \leq \left|\alpha - \frac{p}{q}\right| + \left|\alpha - \frac{P}{Q}\right|$.

(b) Prove that whenever $\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q^2}$ holds true, then $\frac{p}{q}$ is a convergent of α.

Exercise 1.13. Prove Proposition 1.3.21.

1.4 Periodic Continued Fractions and Pell's Equation

We already came across periodic infinite continued fractions, for instance $\langle 1, 1, 1, \ldots \rangle$. A more convenient way to write this, is (as for periodical decimal expansions) $\langle \overline{1} \rangle$.

Example 1.4.1. Which real number α is represented by $\langle \overline{1, 2} \rangle = \langle 1, 2, 1, 2, 1, 2, 1, \ldots \rangle$? Luckily, the most naive thing one could do is the best! We have

$$\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}} = 1 + \frac{1}{2 + \frac{1}{\alpha}} = 1 + \frac{\alpha}{2\alpha + 1}.$$

Multiplying both sides with $(2\alpha+1)$ and shifting everything to one side, yields

$$2\alpha^2 - 2\alpha - 1 = 0.$$

Now we solve this quadratic equation and achieve that α is one of the elements $\frac{1\pm\sqrt{3}}{2}$. But which of them? Since $\alpha = \langle 1, \ldots \rangle$, we know that $1 < \alpha < 2$. This implies $\alpha = \frac{1+\sqrt{3}}{2}$.

Lemma 1.4.2. *Let*

$$\begin{aligned}\alpha &= \langle a_0, a_1, \ldots, a_r, b_1, b_2, \ldots, b_s, b_1, b_2, \ldots, b_s, b_1, \ldots, b_s, b_1, \ldots \rangle \\ &= \langle a_0, \ldots, a_r, \overline{b_1, \ldots, b_s} \rangle\end{aligned}$$

be a periodic infinite continued fraction. Then α is an algebraic number of degree 2.

Proof. The same argument as in Example 1.4.1, proves that $\beta = \langle \overline{b_1, \ldots, b_s} \rangle$ is an algebraic number of degree 2. This is actually all we need to know, since

$$\alpha \overset{1.3.7}{=} \langle a_1, \ldots, a_r, \beta \rangle \overset{1.2.7}{=} \frac{p_r\beta + p_{r-1}}{q_r\beta + q_{r-1}} \in \mathbb{Q}(\beta).$$

Note, that the values p_n, q_n are integers. □

The converse of this lemma is also true:

Theorem 1.4.3. *Let α be an algebraic number of degree 2. Then the continued fraction expansion of α is periodic.*

Proof. By assumption α is a root of a quadratic polynomial with integral coefficients. This is, there are $a, b, c \in \mathbb{Z}$, with

$$a\alpha^2 + b\alpha + c = 0. \tag{1.16}$$

Since α is irrational, there is a unique infinite continued fraction $\langle a_0, a_1, \ldots \rangle$ representing α. This is, as you all know by now, constructed by $a_n = \lfloor \alpha_n \rfloor$, where $\alpha_0 = \alpha$ and $\alpha_n = \frac{1}{\{\alpha_{n-1}\}}$ for all $n \in \mathbb{N}$. How can we read of the periodicity of the continued fraction from the α_n's? Assume that there are $k, \ell \in \mathbb{N}$ with $k \neq \ell$, such that $\alpha_k = \alpha_\ell$, say $\ell = k + r$ for some $r \in \mathbb{N}$. Then we have

$$\begin{aligned}\alpha_{k+r} &= \alpha_\ell = \alpha_k \\ \alpha_{k+r+1} &= \frac{1}{\{\alpha_{k+r}\}} = \frac{1}{\{\alpha_k\}} = \alpha_{k+1} \\ &\vdots \\ \alpha_{k+2r-1} &= \frac{1}{\{\alpha_{k+2r-2}\}} = \frac{1}{\{\alpha_{k+r-2}\}} = \alpha_{k+r-1} \\ \alpha_{k+2r} &= \frac{1}{\{\alpha_{k+2r-1}\}} = \frac{1}{\{\alpha_{k+r-1}\}} = \alpha_{k+r} = \alpha_k.\end{aligned}$$

Now we are in a loop, and it follows

$$a_{n+r} = \lfloor \alpha_{n+r} \rfloor = \lfloor \alpha_n \rfloor = a_n \quad \forall\ n \geq k,$$

which means that the continued fraction is periodic.

We are left to prove that two of the α_n's are equal. The only direct relation between α and α_n that we know is $\alpha = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$ (see Proposition 1.2.7). Hence, by (1.16) it is

$$a \cdot \left(\frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}\right)^2 + b \cdot \left(\frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}\right) + c = 0.$$

Removing denominators yields,

$$A_n\alpha_n^2 + B_n\alpha_n + C_n = 0,$$

with

$$\begin{aligned} A_n &= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 \in \mathbb{Z} \\ B_n &= 2ap_{n-1}q_{n-2} + bp_{n-1}q_{n-2} + bp_{n-2}q_{n-1} + 2cq_{n-1}q_{n-2} \in \mathbb{Z} \\ C_n &= A_{n-1} \in \mathbb{Z}. \end{aligned}$$

We will prove that independently on n, there are only a finite number of possible coefficients A_n, B_n and C_n. So all of the α_n's are roots of a finite number of quadratic polynomials. In particular, there are just finitely many possible values for the α_n, and hence we must have $\alpha_k = \alpha_\ell$ for some $k \neq \ell$.
For any $n \in \mathbb{N}$, by (1.6) we have $\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{q_{n-1}^2}$. Hence, there exists a real r of absolute value < 1 such that $\frac{p_{n-1}}{q_{n-1}} = \alpha + \frac{r}{q_{n-1}^2}$. So finally, we get

$$\begin{aligned} |A_n| &= q_{n-1}^2 \cdot \left| a\left(\frac{p_{n-1}}{q_{n-1}}\right)^2 + b\left(\frac{p_{n-1}}{q_{n-1}}\right) + c \right| \\ &= q_{n-1}^2 \cdot \left| a\left(\alpha + \frac{r}{q_{n-1}^2}\right)^2 + b\left(\alpha + \frac{r}{q_{n-1}^2}\right) + c \right| \quad \text{for some } |r| < 1 \\ &= q_{n-1}^2 \cdot \left| \underbrace{a\alpha^2 + b\alpha + c}_{\overset{(1.16)}{=}0} + 2a\alpha\frac{r}{q_{n-1}^2} + a\frac{r^2}{q_{n-1}^4} + b\frac{r}{q_{n-1}^2} \right| \quad \text{for some } |r| < 1 \\ &= \left| 2a\alpha r + a\frac{r^2}{q_{n-1}^2} + br \right| \leq |2a\alpha r| + \left| a\frac{r^2}{q_{n-1}^2} \right| + |b| \overset{|r|<1}{<} |2a\alpha| + |a| + |b|, \end{aligned}$$

which means that $|A_n|$ is bounded independently on n. Therefore, also $|C_n| = |A_{n-1}|$ is bounded independently on n. We could do some similar estimate for B_n, or we notice that $|B_n| = \sqrt{|4A_nC_n - 4ac + b^2|}$ is bounded independently on n. Since A_n, B_n and C_n are integers, there are only finitely many possible values for the coefficients of the minimal polynomials of the α_n's. As noticed above, this concludes the proof. □

Let us briefly explain the mysterious formula $B_n^2 = 4A_nC_n - 4ac + b^2$. We can represent a quadratic polynomial by a quadratic matrix. Namely, for any $\beta \in \mathbb{C}$ it is

$$\begin{pmatrix} \beta \\ 1 \end{pmatrix}^t \cdot \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \cdot \begin{pmatrix} \beta \\ 1 \end{pmatrix} = a\beta^2 + b\beta + c,$$

and this matrix is uniquely determined by this property. Moreover, for all $\beta \in \mathbb{C}$

$$\begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \cdot \begin{pmatrix} \beta \\ 1 \end{pmatrix} = \begin{pmatrix} p_{n-1}\beta + p_{n-2} \\ q_{n-1}\beta + q_{n-2} \end{pmatrix}.$$

Putting this together, yields for all (but one) $\beta \in \mathbb{C}$

$$\begin{aligned}
&a \cdot \left(\frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}}\right)^2 + b \cdot \left(\frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}}\right) + c \\
&= \left(\frac{1}{q_{n-1}\beta + q_{n-2}} \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \cdot \begin{pmatrix} \beta \\ 1 \end{pmatrix}\right)^t \cdot \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \cdot \left(\frac{1}{q_{n-1}\beta + q_{n-2}} \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \cdot \begin{pmatrix} \beta \\ 1 \end{pmatrix}\right) \\
&= \left(\frac{1}{q_{n-1}\beta + q_{n-2}}\right)^2 \begin{pmatrix} \beta \\ 1 \end{pmatrix}^t \cdot \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}^t \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} \beta \\ 1 \end{pmatrix}.
\end{aligned}$$

On the other hand, by definition of A_n, B_n, C_n we have for all (but one) $\beta \in \mathbb{C}$

$$a \cdot \left(\frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}}\right)^2 + b \cdot \left(\frac{p_{n-1}\beta + p_{n-2}}{q_{n-1}\beta + q_{n-2}}\right) + c = \left(\frac{1}{q_{n-1}\beta + q_{n-2}}\right)^2 \begin{pmatrix} \beta \\ 1 \end{pmatrix}^t \begin{pmatrix} A_n & \frac{B_n}{2} \\ \frac{B_n}{2} & C_n \end{pmatrix} \begin{pmatrix} \beta \\ 1 \end{pmatrix}.$$

Hence, the following equality holds true:

$$\begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}^t \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} = \begin{pmatrix} A_n & \frac{B_n}{2} \\ \frac{B_n}{2} & C_n \end{pmatrix}.$$

Taking determinants yields

$$\begin{aligned}
A_nC_n - \frac{B_n^2}{4} &= \det \begin{pmatrix} A_n & \frac{B_n}{2} \\ \frac{B_n}{2} & C_n \end{pmatrix} = \det \left(\begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}^t \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \right) \\
&= \underbrace{\det \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}}_{=(-1)^{n-2}} \cdot \det \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \cdot \underbrace{\det \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix}}_{=(-1)^{n-2}} = ac - \frac{b^2}{4}.
\end{aligned}$$

This finally implies the claimed relation between B_n, A_n and C_n.

Remark 1.4.4. We are going to use this theory to solve a classical Diophantine equation. Again *Diophantine* refers to the integers. Hence, a Diophantine equation is usually given by a $F \in \mathbb{Z}[x_1, \ldots, x_n]$ and one is interested in finding $a_1, \ldots, a_n \in \mathbb{Z}$ satisfying $F(a_1, \ldots, a_n) = 0$. In general, it is even too hard to decide whether such a solution exists, and if, if there are infinitely many solutions.

Definition 1.4.5. Let $d \in \mathbb{N}$ be arbitrary, then the equation

$$x^2 - dy^2 = 1 \tag{1.17}$$

is called *Pell's equation*. A *solution* to Pell's equation is a pair $(x, y) \in \mathbb{Z}^2$, such that (1.17) is satisfied.

This equation is named after John Pell (1611–1685), who never wrote anything concerning this equation.

Remark 1.4.6. It is easy to see that there are only two solutions to (1.17) if d is a square number. So we assume from now on that $\sqrt{d} \in \mathbb{R} \setminus \mathbb{Q}$. If (x, y) is a solution to (1.17), then $\frac{1}{y^2} = \frac{x^2}{y^2} - d$. For large y, this implies that $\frac{x}{y}$ is close to $\sqrt{d}$. So morally approximations of $\sqrt{d}$ should be connected to solutions of (1.17).
From number theory, you know Dirichlet's unit theorem. This tells you that the unit group of $\mathbb{Z} + \sqrt{d}\mathbb{Z}$ is multiplicatively generated by -1 and some fundamental unit ϵ (note that $\mathbb{Z} + \sqrt{d}\mathbb{Z}$ is an order in the field $\mathbb{Q}(\sqrt{d})$). Write $\epsilon = a + \sqrt{d}b$ for some $a, b \in \mathbb{Z}$, $b \neq 0$. Since ϵ is a unit, the norm of ϵ satisfies $a^2 - db = \pm 1$. The norm is multiplicative, and hence the norm of $\epsilon^{2n} = a_n + \sqrt{d}b_n$ is 1. This implies that for all $n \in \mathbb{N}$ the pair (a_n, b_n) is a solution of (1.17). In particular, Pell's equation has infinitely many solutions. We will use continued fractions, to explicitly construct solutions of Pell's equation.

Proposition 1.4.7. *Let $d \in \mathbb{N}$ be not a square. Then there is an $s \in \mathbb{N}$ such that*

$$\sqrt{d} = \langle a_0, \overline{a_1, \dots, a_s} \rangle.$$

Proof. We use our good friends $\alpha_0, \alpha_1, \dots$ Recall that $\alpha = \langle a_0, \dots, a_{n-1}, \alpha_n \rangle$, and $\alpha_{n+1} = \frac{1}{\alpha_n - a_n} \in \mathbb{Q}(\sqrt{d})$ for all $n \in \mathbb{N}$. Manipulating this equation gives $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$ for all $n \in \mathbb{N}$. Let σ be the non-trivial element in $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$; i.e. $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$ for all $a, b \in \mathbb{Q}$. Then

$$\begin{aligned} & \sigma(\alpha_1) = \sigma\left(\frac{1}{\sqrt{d} - \lfloor \sqrt{d} \rfloor}\right) = \frac{1}{-\sqrt{d} - \lfloor \sqrt{d} \rfloor} \in (-1, 0) \\ \implies \quad & \sigma(\alpha_2) = \sigma\left(\frac{1}{\alpha_1 - a_1}\right) = \frac{1}{\sigma(\alpha_1) - a_1} \in (-1, 0) \\ \overset{\text{induction}}{\implies} \quad & \sigma(\alpha_n) \in (-1, 0) \quad \forall\ n \in \mathbb{N}. \end{aligned} \tag{1.18}$$

By Theorem 1.4.3 we know that $\alpha = \langle a_0, \dots, a_k, \overline{a_{k+1}, \dots, a_{k+r}} \rangle$ for some $k, r \in \mathbb{N}$. Assume that k is minimal with this property, and $k > 1$. Then, we have

$$a_k \neq a_{k+r}, \tag{1.19}$$

since otherwise $\alpha = \langle a_0, \dots, a_{k-1}, \overline{a_k, \dots, a_{k+r-1}} \rangle$, contradicting the minimality (here we need the assumption $k > 1$). Moreover, (see Remark 1.3.7)

$$\alpha_{k+1} = \langle \overline{a_{k+1}, \dots, a_{k+1+r}} \rangle = \alpha_{k+r+1}. \tag{1.20}$$

On the other hand, we have

$$\underbrace{\underbrace{\sigma(\alpha_k)}_{\overset{(1.18)}{\in}(-1,0)} - \underbrace{\sigma(\alpha_{k+r})}_{\overset{(1.18)}{\in}(-1,0)}}_{\in(-1,1)} = \sigma(\alpha_k - \alpha_{k+r})$$

$$= \sigma\left(a_k + \frac{1}{\alpha_{k+1}} - a_{k+r} - \frac{1}{\alpha_{k+r+1}}\right) \overset{(1.20)}{=} \sigma(\underbrace{a_k - a_{k+r}}_{\in\mathbb{Z}}) = a_k - a_{k+r}.$$

Hence, $a_k - a_{k+r}$ is an integer in $(-1, 1)$, which contradicts (1.19). It follows that $k \leq 1$ and hence $\sqrt{d} = \langle a_0, \overline{a_1, \dots, a_{r+1}} \rangle$. □

Finally we can solve Pell's equation.

Theorem 1.4.8. *Let $d \in \mathbb{N}$ be not a square, with $\sqrt{d} = \langle a_0, \overline{a_1, \dots, a_r} \rangle$. As usual $\frac{p_n}{q_n}$ denotes the n-th convergent of $\sqrt{d}$. For all $k \in \mathbb{N}_0$ we have*

$$p_{kr-1}^2 - d q_{kr-1}^2 = (-1)^{kr-2}.$$

In particular, at latest the $(2r-2)$-nd convergent of $\sqrt{d}$ gives a non-trivial solution for Pell's equation (1.17).

Proof. We use the notation from the proof above. Since all arguments are familiar by now, we can rush through the proof. For all $k \in \mathbb{N}$ we have

$$\frac{1}{\sqrt{d}-a_0} = \alpha_1 = \langle \overline{a_1, \ldots, a_r} \rangle = \alpha_{kr+1}.$$

Fix any $k \in \mathbb{N}_0$ and set $x = a_{kr} - a_0 \in \mathbb{Z}$. Then $\alpha_{kr} = a_{kr} + \frac{1}{\alpha_{kr+1}} = x + \sqrt{d}$.

$$\begin{aligned}
&\overset{1.2.7}{\Longrightarrow} \quad \sqrt{d} = \frac{p_{kr-1}\alpha_{kr} + p_{kr-2}}{q_{kr-1}\alpha_{kr} + q_{kr-2}} = \frac{(x+\sqrt{d})p_{kr-1} + p_{kr-2}}{(x+\sqrt{d})q_{kr-1} + q_{kr-2}} \\
&\Longrightarrow \quad dq_{kr-1} + (xq_{kr-1} + q_{kr-2})\sqrt{d} = (xp_{kr-1} + p_{kr-2}) + p_{kr-1}\sqrt{d} \\
&\Longrightarrow \quad dq_{kr-1} = xp_{kr-1} + p_{kr-2} \quad \& \quad xq_{kr-1} + q_{kr-2} = p_{kr-1} \\
&\Longrightarrow \quad dq_{kr-1}^2 = xp_{kr-1}q_{kr-1} + p_{kr-2}q_{kr-1} \quad \& \quad xq_{kr-1}p_{kr-1} + q_{kr-2}p_{kr-1} = p_{kr-1}^2 \\
&\Longrightarrow \quad p_{kr-1}^2 - dq_{kr-1}^2 = p_{kr-1}q_{kr-2} - q_{kr-1}p_{kr-2} \overset{1.2.2}{=} (-1)^{kr-2}.
\end{aligned}$$

This proves the proposition. □

Exercises

Exercise 1.14. Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Give formulas for the quadratic algebraic numbers $\langle \overline{a} \rangle$ and $\langle b, \overline{a} \rangle$.

Exercise 1.15. Let $d \in \mathbb{N}$ be arbitrary. Prove the following statements:

(a) If d is a square number, then there are just two integral solutions of $x^2 - dy^2 = 1$.

(b) If d is not a square number, and $p, q \in \mathbb{N}$ are such that $p^2 - dq^2 = 1$, then $\frac{p}{q}$ is a convergent of $\sqrt{d}$.

Hint: Exercise 1.12.

Chapter 2

The Weil-Height

2.1 The Mahler Measure

We want to formulate Roth's Theorem 1.1.17 for an arbitrary number field. Recall, that Roth's theorem for $\mathbb{Q}$ reads:

$$\forall\ \alpha \in \overline{\mathbb{Q}},\ \forall\ \varepsilon > 0,\ \exists\ c(\alpha,\varepsilon) > 0,\ \text{such that}\ \left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha,\varepsilon)}{|q|^{2+\varepsilon}},\quad \forall\ \frac{p}{q} \in \mathbb{Q} \setminus \{\alpha\}. \tag{RT1}$$

(I know that this does not look very nice, but we need to have the whole statement in one line for later references.) Note that this is not precisely the same formulation as in Theorem 1.1.17. But we have simply avoided any assumption on p and q in $\mathbb{Z}$, which explains the usage of $|q|$ instead of q. Moreover, if $\alpha \in \mathbb{Q}$, then the only good rational approximation of α is α itself (cf. Lemma 1.1.4). However, we still use the explicit form $\frac{p}{q}$ with $p, q \in \mathbb{Z}$ for an rational number. Such a nice representation is not available in an arbitrary number field K. We now come to another mild reformulation of (RT1).

Lemma 2.1.1. *Roth's Theorem* (RT1) *is equivalent to the following statement: For all $\alpha \in \overline{\mathbb{Q}}$ and for all $\varepsilon > 0$ there exists a positive constant $c(\alpha,\varepsilon) > 0$ such that $\left|\alpha - \frac{p}{q}\right| > c(\alpha,\varepsilon) \cdot \max\{|p|, |q|\}^{-(2+\varepsilon)}$ for all $\frac{p}{q} \in \mathbb{Q} \setminus \{\alpha\}$. Formally this statement reads*

$$\forall\ \alpha \in \overline{\mathbb{Q}},\ \forall\ \varepsilon > 0,\ \exists\ c(\alpha,\varepsilon) > 0,\ \textit{such that}\quad \left|\alpha - \frac{p}{q}\right| > c(\alpha,\varepsilon) \cdot \max\{|p|, |q|\}^{-(2+\varepsilon)},\quad \forall\ \frac{p}{q} \in \mathbb{Q} \setminus \{\alpha\}. \tag{RT2}$$

Proof. We prove the two necessary implications.

$\Rightarrow$ This implication follows immediately, since for all $\frac{p}{q} \in \mathbb{Q} \setminus \{\alpha\}$ we have

$$\left|\alpha - \frac{p}{q}\right| \overset{\text{(RT1)}}{>} \frac{c(\alpha,\varepsilon)}{|q|^{2+\varepsilon}} = c(\alpha,\varepsilon) \cdot |q|^{-(2+\varepsilon)} \geq c(\alpha,\varepsilon) \cdot \max\{|p|, |q|\}^{-(2+\varepsilon)}.$$

$\Leftarrow$ We first note that for any $n \in \mathbb{Z}$ we have $\left|\alpha - \frac{p}{q}\right| = \left|(\alpha + n) - \frac{p+nq}{q}\right|$ for all $\frac{p}{q} \in \mathbb{Q}$. This means that shifting α by an integer, does not affect the possible approximations

by rational numbers. In particular, for fixed $\alpha \in \overline{\mathbb{Q}}$, and fixed $\varepsilon, c > 0$ we have

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{|q|^{2+\varepsilon}} \quad \forall\, \frac{p}{q} \in \mathbb{Q}\backslash\{\alpha\} \quad \Longleftrightarrow \quad \left|\underbrace{(\alpha - \lfloor\alpha\rfloor)}_{\in(0,1)} - \frac{p}{q}\right| > \frac{c}{|q|^{2+\varepsilon}} \quad \forall\, \frac{p}{q} \in \mathbb{Q}\backslash\{\alpha - \lfloor\alpha\rfloor\}.$$

Hence, in order to prove (RT1) we may and will assume from now on that $\alpha \in [0,1) \cap \overline{\mathbb{Q}}$. If $|p| > |q|$, then

$$\left|\alpha - \frac{p}{q}\right| \geq \left|\underbrace{|\alpha|}_{\in[0,1)} - \underbrace{\left|\frac{p}{q}\right|}_{\geq \frac{|q|+1}{|q|}}\right| \geq \frac{|q|+1}{|q|} - 1 = \frac{1}{|q|} = \frac{|q|^{1+\varepsilon}}{|q|^{2+\varepsilon}} \geq \frac{1}{|q|^{2+\varepsilon}}.$$

Hence, for any $\varepsilon > 0$ there exists a $c(\alpha, \varepsilon) > 0$ such that for all $\frac{p}{q} \in \mathbb{Q} \setminus \{\alpha\}$ we have

$$\left|\alpha - \frac{p}{q}\right| > \begin{cases} \frac{1}{|q|^{2+\varepsilon}} & \text{if } |p| > |q| \\ \frac{c(\alpha,\varepsilon)}{|q|^{2+\varepsilon}} & \text{if } |p| \leq |q| \text{ (by (RT2))} \end{cases}$$

But this just means, that for all $\frac{p}{q} \in \mathbb{Q} \setminus \{\alpha\}$ we have $\left|\alpha - \frac{p}{q}\right| > \frac{\min\{1, c(\alpha,\varepsilon)\}}{|q|^{2+\varepsilon}}$, implying (RT1).

□

Definition 2.1.2. Let $\alpha \in \overline{\mathbb{Q}}$ be arbitrary and let $f(x) \in \mathbb{Z}[x]$ be a minimal polynomial of α. Write $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0 = a_d(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_d)$; i.e. $a_0, \ldots, a_d \in \mathbb{Z}$ and $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ are the roots of $f(x)$. Then the *Mahler measure* of α is given by

$$M(\alpha) = |a_d| \cdot \prod_{i=1}^{d} \max\{1, |\alpha_i|\}.$$

Remark 2.1.3.

- Recall that a minimal polynomial $f(x) = a_d x^d + \ldots + a_0$ of α is irreducible in $\mathbb{Z}[x]$ (so in particular it is irreducible in $\mathbb{Q}[x]$). Moreover, the greatest common divisor of $a_0, \ldots, a_d$ is 1. It follows that $-f(x)$ is the only other minimal polynomial of α, hence the Mahler measure of α is well defined.

- The Mahler measure of α is just the absolute value of the product of the leading coefficient of f and all roots of f lying outside the unit circle. In particular, $M(\alpha) \geq 1$ for all $\alpha \in \overline{\mathbb{Q}}$.

- The elements $\alpha_1, \ldots, \alpha_d$ from the definition of the Mahler measure are precisely the Galois conjugates of α (including α itself). We conclude that $M(\alpha) = M(\sigma(\alpha))$ for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Example 2.1.4. Let us calculate a few examples.

(a) Let $p, q \in \mathbb{Z}$, with $q \neq 0$ and $\gcd(p,q) = 1$. Then the minimal polynomial of $\frac{p}{q}$ is $qx - p$. Hence,

$$M(\frac{p}{q}) = |q| \cdot \max\{1, \left|\frac{p}{q}\right|\} = \max\{|q|, |q| \cdot \left|\frac{p}{q}\right|\} = \max\{|q|, |p|\}.$$

(Haven't we seen this maximum before?!)

(b) The minimal polynomial of $\sqrt{2}$ is $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. Hence,

$$M(\sqrt{2}) = |1| \cdot \left|\sqrt{2}\right| \cdot \left|-\sqrt{2}\right| = 2.$$

(c) The minimal polynomial of the golden ratio $\frac{1+\sqrt{5}}{2}$ is $x^2 - x - 1 = (x - \frac{1+\sqrt{5}}{2})(x - \frac{1-\sqrt{5}}{2})$. Hence,

$$M(\frac{1+\sqrt{5}}{2}) = \frac{1+\sqrt{5}}{2}.$$

By this example, Roth's theorem (RT2) can be formulated as: For all $\alpha \in \overline{\mathbb{Q}}$ and all $\varepsilon > 0$, there exists a positive constant $c(\alpha, \varepsilon) > 0$ such that $|\alpha - \beta| > c(\alpha, \varepsilon) \cdot M(\beta)^{-(2+\varepsilon)}$ for all $\beta \in \mathbb{Q} \setminus \{\alpha\}$. Formally,

$$\forall\ \alpha \in \overline{\mathbb{Q}},\ \forall\ \varepsilon > 0,\ \exists\ c(\alpha, \varepsilon) > 0,\ \text{such that}\ |\alpha - \beta| > c(\alpha, \varepsilon) \cdot M(\beta)^{-(2+\varepsilon)}, \quad \forall\ \beta \in \mathbb{Q} \setminus \{\alpha\}. \tag{RT3}$$

In this formulation, $\mathbb{Q}$ could be replaced by any number field, since every algebraic number has a Mahler measure! So let us study this measure further.

Lemma 2.1.5 (Vieta's formula)**.** *Let $a_d, \alpha_1, \ldots, \alpha_d \in \mathbb{C}$ be arbitrary, with $a_d \neq 0$. Then*

$$a_d(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_d) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0,$$

with

$$a_i = (-1)^{d-i} \cdot a_d \cdot \sum_{\substack{J \subseteq \{1,\ldots,d\} \\ |J| = d-i}} \left(\prod_{j \in J} \alpha_j \right) \quad \forall\ i \in \{0, \ldots, d\}.$$

Proof. This is well known and easy to see: If we multiply the left hand side, then choosing the x precisely i-times, is the same as choosing $d - i$ of the values $\alpha_1, \ldots, \alpha_d$. Since the a_i is the sum of all these choices, the Lemma follows. □

Remark 2.1.6. An $\alpha \in \overline{\mathbb{Q}}$ is called an algebraic *integer* if the minimal polynomial of α in $\mathbb{Z}[x]$ is monic; i.e. the minimal polynomial of α is of the form $x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$. The set of algebraic integers in a number field K is a ring, which we will denote by $\mathcal{O}_K$.

Lemma 2.1.7. *Let $\alpha \in \overline{\mathbb{Q}}$ be of degree d and let $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Z}[x]$ be a minimal polynomial of α. Then for all $i \in \{0, \ldots, d\}$ we have*

$$\binom{d}{i} M(\alpha) \geq |a_i|.$$

Proof. Let $\alpha_1, \ldots, \alpha_d$ be the roots of f; i.e. the Galois conjugates of α. For any $i \in \{0, \ldots, d\}$ Vieta's formula 2.1.5 implies

$$|a_i| = |a_d| \cdot \sum_{\substack{J \subseteq \{1,\ldots,d\} \\ |J| = d-i}} \left(\prod_{j \in J} |\alpha_j| \right) \leq |a_d| \cdot \sum_{\substack{J \subseteq \{1,\ldots,d\} \\ |J| = d-i}} \left(\prod_{j=1}^{d} \max\{1, |\alpha_j|\} \right)$$

$$= \sum_{\substack{J \subseteq \{1,\ldots,d\} \\ |J| = d-i}} \underbrace{\left(|a_d| \cdot \prod_{j=1}^{d} \max\{1, |\alpha_j|\} \right)}_{= M(\alpha)} = \binom{d}{d-i} M(\alpha) = \binom{d}{i} M(\alpha).$$

□

Theorem 2.1.8 (Northcott)**.** *Let $A, B \in \mathbb{R}$ be arbitrary. Then there are at most finitely many algebraic numbers $\alpha \in \overline{\mathbb{Q}}$ with $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq A$ and $M(\alpha) \leq B$.*

Proof. We need to prove that the set

$$\{\alpha \in \overline{\mathbb{Q}} | [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq A, \text{ and } M(\alpha) \leq B\} = \bigcup_{1 \leq d \leq A} \{\alpha \in \overline{\mathbb{Q}} | [\mathbb{Q}(\alpha) : \mathbb{Q}] = d, \text{ and } M(\alpha) \leq B\}$$

is finite. Hence it is enough to prove the finiteness of

$$\{\alpha \in \overline{\mathbb{Q}} | [\mathbb{Q}(\alpha) : \mathbb{Q}] = d, \text{ and } M(\alpha) \leq B\}$$

for fixed $d \in \mathbb{N}$. But if $\alpha \in \overline{\mathbb{Q}}$ is of degree d, then its minimal polynomial is of the form $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Z}[x]$, with $a_d \neq 0$. If also $M(\alpha) \leq B$, then by Lemma 2.1.7

$$|a_i| \leq \binom{d}{i} M(\alpha) \leq \binom{d}{i} \cdot B \quad \forall\, i \in \{0, \ldots, d\}.$$

Hence, since $a_i \in \mathbb{Z}$, there are just finitely many possible coefficients for the minimal polynomial of an algebraic α of degree d and Mahler measure $\leq B$. This implies that there are only finitely such algebraic numbers, concluding the proof. □

Remark 2.1.9. Northcott's theorem tells us in particular that $\{\alpha \in K | M(\alpha) \leq B\}$ is finite for any number fields K and all $B \in \mathbb{R}$. This means that one can use the Mahler measure to count elements in a number field, and to prove finiteness results in number fields. The latter statement can be explained as follows, if we want to prove that a certain set of points in an number field K is finite, we need to prove that the Mahler measure of each element of the set is uniformly bounded from above.
This explains the reason for taking $\max\{1, |\alpha_i|\}$ instead of $|\alpha_i|$ in the definition of the Mahler measure. In the latter case, at least for algebraic integers, we would get the modulus of the usual *norm*. But surely there may be infinitely many algebraic integers of bounded norm in a number field. For instance, algebraic units $\alpha \in \mathcal{O}_K^*$ have norm ± 1, but there are infinitely many algebraic units in K, as long as K is neither $\mathbb{Q}$ nor a totally imaginary quadratic field.

Lemma 2.1.10. *A polynomial $f(x) = a_d x^d + \ldots + a_0 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, if and only if $f(x)$ is irreducible in $\mathbb{Q}[x]$ and $\gcd(a_0, \ldots, a_d) = 1$.*

Proof. This is usually proved in an algebra course. □

Proposition 2.1.11. *The following statements are true:*

(i) $M(\alpha) = M(\alpha^{-1})$ *for all* $\alpha \in \overline{\mathbb{Q}}^*$, *and*

(ii) $M(\alpha^k) \leq M(\alpha)^k$ *for all* $k \in \mathbb{N}$ *and all algebraic integers* α.

(The assumption in (ii) that α *has to be an algebraic integer instead of an arbitrary algebraic number, will be removed soon.)*

Proof. Let α be an algebraic number of degree $d \in \mathbb{N}$ with minimal polynomial

$$f(x) = a_d x^d + \ldots + a_0 = a_d(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_d) \in \mathbb{Z}[x].$$

(i) To prove the claimed equality, we want to express the minimal polynomial of α^{-1} in terms of $f(x)$. We know from algebra, that the degree of the minimal polynomial of α^{-1} is equal to $\deg(f) = d$. Hence, by Lemma 2.1.10 a polynomial $g(x) \in \mathbb{Z}[x]$ is a minimal polynomial of α^{-1} if and only if $\deg(g) = d$, $g(\alpha^{-1}) = 0$, and the gcd of all the coefficients of g is one.

We note that

$$g(x) = x^d f(\frac{1}{x}) = x^d \cdot (a_d(\frac{1}{x})^d + a_{d-1}(\frac{1}{x})^{d-1} + \ldots + a_0) = a_d + a_{d-1}x + \ldots + a_0 x^d \in \mathbb{Z}[x]$$

satisfies all these conditions: Since $f(\alpha) = 0$, we have $g(\alpha^{-1}) = \alpha^{-d} f(\alpha) = 0$. Moreover, the irreducibility of $f(x)$ implies $a_0 \neq 0$, since otherwise x would be a divisor of $f(x)$. Hence, $\deg(g) = d$. Lastly, again be the irreducibility of f, one has $\gcd(a_0, \ldots, a_d) = 1$ (note that the coefficients of f and g are the same in reversed order).

So now we know the minimal polynomial of α^{-1} and we know that the roots of $g(x)$ are precisely $\frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_d}$ (which follows already immediately by Galois theory). Hence,

$$\begin{aligned} M(\alpha^{-1}) &= |a_0| \cdot \prod_{i=1}^{d} \max\left\{1, \left|\frac{1}{|\alpha_i|}\right|\right\} \overset{2.1.5}{=} |a_d| \cdot \prod_{i=1}^{d} |\alpha_i| \cdot \prod_{i=1}^{d} \max\left\{1, \left|\frac{1}{|\alpha_i|}\right|\right\} \\ &= |a_d| \cdot \prod_{i=1}^{d} |\alpha_i| \cdot \max\left\{1, \left|\frac{1}{|\alpha_i|}\right|\right\} = |a_d| \cdot \prod_{i=1}^{d} \max\left\{|\alpha_i|, \left||\alpha_i| \cdot \frac{1}{|\alpha_i|}\right|\right\} \\ &= |a_d| \cdot \prod_{i=1}^{d} \max\{|\alpha_i|, 1\} = M(\alpha). \end{aligned}$$

This proves (i).

(ii) From now on we assume that α is an algebraic *integer*. Then, since $a_d = 1$, it is $M(\alpha) = \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$. The only possible Galois conjugates of α^k are $\alpha_1^k, \ldots, \alpha_d^k$. Say, the Galois conjugates of α^k are precisely $\{\alpha_i^k | i \in I\}$ for some $I \subseteq \{1, \ldots, d\}$. Since α^k is again an algebraic integer, we find

$$M(\alpha^k) = \prod_{i \in I} \max\{1, \left|\alpha_i^k\right|\} \leq \prod_{i=1}^{d} \max\{1, \left|\alpha_i^k\right|\} = \prod_{i=1}^{d} \max\{1, |\alpha_i|\}^k = M(\alpha)^k.$$

□

Theorem 2.1.12 (Kronecker)**.** *For $\alpha \in \overline{\mathbb{Q}}^*$ we have $M(\alpha) = 1$ if and only if α is a root of unity.*

Remark 2.1.13. Recall that $M(\alpha) \geq 1$ for all $\alpha \in \overline{\mathbb{Q}}$. Hence, Kronecker's theorem tells us that the Mahler measure is minimal precisely for roots of unity.

Proof of Theorem 2.1.12. We use the usual notation for the minimal polynomial of α. Then $M(\alpha) = |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\} = 1$ if and only if $|a_d| = 1$ and $\max\{1, |\alpha_i|\} = 1$ for all $i \in \{1, \ldots, d\}$. In particular, this is the case if and only if α is an algebraic *integer* such that all Galois conjugates lie on or inside the unit circle.[1]
If α is a root of unity, then the minimal polynomial of α is a divisor of $x^n - 1$ for some $n \in \mathbb{N}$. In particular, the leading coefficient is one (i.e. α is an algebraic integer) and all roots lie on the unit circle. Hence, $M(\alpha) = 1$ as noted above.
Now, assume that $M(\alpha) = 1$. Then, α must be an algebraic integer. Moreover, for any $k \in \mathbb{N}$ we have

$$1 \leq M(\alpha^k) \overset{2.1.11}{\leq} M(\alpha)^k = 1,$$

which implies $M(\alpha^k) = 1$ for all $k \in \mathbb{N}$. Moreover, $\alpha^k \in \mathbb{Q}(\alpha)$ for all $k \in \mathbb{N}$. Hence, by Northcott's theorem the set $\alpha, \alpha^2, \alpha^3, \alpha^4, \ldots$ is finite! Therefore, it exist $k, \ell \in \mathbb{N}$, with $k > \ell$ and $\alpha^k = \alpha^\ell$. We conclude $\alpha^{k-\ell} = 1$, and hence α is a root of unity. □

Remark 2.1.14. This means that any algebraic *integer* with all its Galois conjugates on the unit circle, must be a root of unity. Without this integral assumption this is false. The number $\frac{2+i}{2-i}$ surely has all Galois conjugates on the unit circle, but it is note a root of unity. Also notice that its minimal polynomial is $5x^2 - 6x + 5$ and hence $M(\frac{2+i}{2-i}) = 5$.

The (in my personal biased opinion) main conjecture concerning the Mahler measure is the following.

Lehmer's conjecture 2.1.15. *There exists an absolute constant $c > 1$, such that $M(\alpha) \geq c$ for all $\alpha \in \overline{\mathbb{Q}}^*$ which are not a root of unity.*
More precisely, the constant c is conjectured to be $1,1762\ldots$, the Mahler measure of any root of

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1.$$

Remark 2.1.16. Actually D. H. Lehmer never conjectured anything. He found in 1933 [7] that the Mahler measure of a root of this polynomial is remarkably small, and he then asked if there is an irreducible polynomial leading to a smaller value than c. Such a polynomial has not been found, yet. This is somehow amazing, comparing the computational power of today and of 1933...

There is another, more analytic, definition of the Mahler measure. Let us recall the *mean value theorem for harmonic functions*, at least a very special case of it: If $g : \mathbb{C} \to \mathbb{R}$ is harmonic in the unit disc $D = \{z \in \mathbb{Z} | z \leq 1\}$, then the mean value of g on the unit circle is equal to $g(0)$; i.e. $g(0) = \frac{1}{2\pi} \int_0^{2\pi} g(e^{i\theta}) \mathrm{d}\theta$.

Proposition 2.1.17. *Let $f(x) = a_d x^d + \ldots + a_0 = a_d(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_d) \in \mathbb{Z}[x]$ be irreducible. That is, $f(x)$ is the minimal polynomial of α_i for all $i \in \{1, \ldots, d\}$. Then*

$$M(\alpha_1) = \exp\left(\frac{1}{2\pi} \int_0^{2\pi} \log\left|f(e^{i\theta})\right| \mathrm{d}\theta\right).$$

[1] From Lemma 2.1.5 it follows, that actually all roots must lie *on* the unit circle.

Proof. We first note that

$$\begin{aligned}
\exp\left(\frac{1}{2\pi}\int_0^{2\pi}\log\left|f(e^{i\theta})\right|\mathrm{d}\theta\right) &= \exp\left(\frac{1}{2\pi}\int_0^{2\pi}\log\left|a_d(e^{i\theta}-\alpha_1)\cdot\ldots\cdot(e^{i\theta}-\alpha_d)\right|\mathrm{d}\theta\right)\\
&= \exp\left(\frac{1}{2\pi}\int_0^{2\pi}\log|a_d| + \sum_{k=1}^{d}\log\left|e^{i\theta}-\alpha_k\right|\mathrm{d}\theta\right)\\
&= \exp\left(\underbrace{\frac{1}{2\pi}\int_0^{2\pi}\log|a_d|\,\mathrm{d}\theta}_{=\log|a_d|} + \sum_{k=1}^{d}\frac{1}{2\pi}\int_0^{2\pi}\log\left|e^{i\theta}-\alpha_k\right|\mathrm{d}\theta\right)\\
&= |a_d|\cdot\prod_{k=1}^{d}\exp\left(\frac{1}{2\pi}\int_0^{2\pi}\log\left|e^{i\theta}-\alpha_k\right|\mathrm{d}\theta\right) \qquad (2.1)
\end{aligned}$$

For any $\alpha\in\mathbb{C}$ with $|\alpha|>1$, the function $\log|x-\alpha|$ is harmonic on the unit disc. Hence, in this case we have $\frac{1}{2\pi}\int_0^{2\pi}\log\left|e^{i\theta}-\alpha\right|\mathrm{d}\theta = \log|0-\alpha| = \log|\alpha| > 0$, by the mean value theorem.
For any $\alpha\in\mathbb{C}$ with $|\alpha|<1$, the function $\log|1-\overline{x}\alpha|$ is harmonic on the unit disc. Moreover, for any z on the unit circle, we have $\log|z-\alpha| = \log(|z|\cdot|1-\overline{z}\alpha|)$. Hence, again by the mean value theorem, we have

$$\frac{1}{2\pi}\int_0^{2\pi}\log\left|e^{i\theta}-\alpha\right|\mathrm{d}\theta = \frac{1}{2\pi}\int_0^{2\pi}\log\left|1-e^{-i\theta}\alpha\right|\mathrm{d}\theta = \log(1) = 0.$$

Finally, for any $\alpha\in\mathbb{C}$ on the unit circle, let $z_1, z_2, \ldots$ be a sequence of complex numbers in the unit circle, converging to α. Then,

$$\frac{1}{2\pi}\int_0^{2\pi}\log\left|e^{i\theta}-\alpha\right|\mathrm{d}\theta = \frac{1}{2\pi}\int_0^{2\pi}\log\left|e^{i\theta}-\lim_{n\to\infty}z_n\right|\mathrm{d}\theta = \lim_{n\to\infty}\frac{1}{2\pi}\int_0^{2\pi}\log\left|e^{i\theta}-z_n\right|\mathrm{d}\theta = 0.$$

Hence, for any $\alpha\in\mathbb{C}$ we have $\frac{1}{2\pi}\int_0^{2\pi}\log\left|e^{i\theta}-\alpha\right|\mathrm{d}\theta = \max\{0,\log|\alpha|\}$. Now we can proceed with equation 2.1, concluding

$$\begin{aligned}
\exp\left(\frac{1}{2\pi}\int_0^{2\pi}\log\left|f(e^{i\theta})\right|\mathrm{d}\theta\right) &= |a_d|\cdot\prod_{k=1}^{d}\exp\left(\frac{1}{2\pi}\int_0^{2\pi}\log\left|e^{i\theta}-\alpha_k\right|\mathrm{d}\theta\right)\\
&= |a_d|\cdot\prod_{k=0}^{d}\exp\left(\max\{0,\log|\alpha_k|\}\right)\\
&= |a_d|\cdot\prod_{k=0}^{d}\max\{1,|\alpha_k|\} = M(\alpha_1).
\end{aligned}$$

□

We will now slowly come back to our original goal, namely to generalize the results from Section 1.1. But before we do so, we will learn a further technicality.

Definition 2.1.18. Let R be a ring. Moreover, let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ and $g(x) = b_k x^k + b_{k-1}x^{k-1} + \ldots + b_0$ be two polynomials in $R[x]$. The *resultant of f and g* is the determinant of the $(n+k) \times (n+k)$-matrix

$$\left.\begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & a_n & \cdots & a_1 & a_0 & 0 & \ldots & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ldots & \ldots & \vdots \\ 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & \cdots & a_0 & 0 \\ 0 & \cdots & 0 & 0 & a_n & a_{n-1} & \cdots & \cdots & a_0 \\ b_k & b_{k-1} & \cdots & b_1 & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & b_k & \cdots & \cdots & b_1 & b_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ldots & \ldots & \vdots \\ 0 & \cdots & 0 & b_k & b_{k-1} & \cdots & \cdots & b_0 & 0 \\ 0 & \cdots & 0 & 0 & b_k & b_{k-1} & \cdots & \cdots & b_0 \end{pmatrix}\right\}\begin{matrix} \\ \\ \\ \\ \\ k \\ \\ \\ \\ \\ n \end{matrix} \tag{2.2}$$

The resultant of f and g is denoted by $\mathrm{Res}(f,g) \in R$.

Example 2.1.19. The resultant of $f(x) = x^2+2x+3 \in \mathbb{Z}[x]$ and $g(x) = -4x^3-3x^2-2x-1 \in \mathbb{Z}[x]$ is the determinant of

$$\begin{pmatrix} 1 & 2 & 3 & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 \\ 0 & 0 & 1 & 2 & 3 \\ -4 & -3 & -2 & -1 & 0 \\ 0 & -4 & -3 & -2 & -1 \end{pmatrix}$$

I just wanted to illustrate the form of the matrix, but for completeness we note that $\mathrm{Res}(f,g) = 256$.

Theorem 2.1.20. *Let $x_1, \ldots, x_n, y_1, \ldots, y_k$ be distinct formal variables over the integral domain R'. We define the polynomial ring $R = R'[x_1, \ldots, x_n, y_1, \ldots, y_k]$ in $n+k$ variables. Let $a_0, \ldots, a_n, b_0, \ldots, b_k \in R$, $a_n \neq 0 \neq b_k$, be such that*

$$a_n(T-x_1)\cdot\ldots\cdot(T-x_n) = a_nT^n + a_{n-1}T^{n-1} + \ldots + a_0 = f(T) \in R[T], \text{ and} \tag{2.3}$$

$$b_k(T-y_1)\cdot\ldots\cdot(T-y_k) = b_kT^k + b_{k-1}T^{k-1} + \ldots + b_0 = g(T) \in R[T]. \tag{2.4}$$

Then

$$\mathrm{Res}(f,g) = a_n^k b_k^n \prod_{i=1}^{n}\prod_{j=1}^{k}(x_i - y_j) \in R.$$

Proof. Since a polynomial ring over an integral domain is again an integral domain, the ring R is again an integral domain. Moreover, for any $a_n, b_k \in R \setminus \{0\}$ there are uniquely determined elements $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{k-1}$ satisfying (2.3) and (2.4). We just have to calculate the left hand sides of (2.3) and (2.4) and collect the T's of the same exponent.
The claimed formula for the resultant looks like a Vandermonde-determinant. So it may not surprise you, that a Vandermonde-matrix appears in the proof. Define

$$V = \begin{pmatrix} y_1^{n+k-1} & \cdots & y_k^{n+k-1} & x_1^{n+k-1} & \cdots & x_n^{n+k-1} \\ y_1^{n+k-2} & \cdots & y_k^{n+k-2} & x_1^{n+k-2} & \cdots & x_n^{n+k-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ y_1^0 & \cdots & y_k^0 & x_1^0 & \cdots & x_n^0 \end{pmatrix}$$

and denote the matrix from (2.2) by S (the matrix is known as a *Sylvester*-matrix). Then, using the well-known formula for the Vandermonde-determinant[2],

$$\det(S \cdot V) = \det(S) \cdot \det(V) \overset{2.1.18}{=} \operatorname{Res}(f,g) \cdot \det(V) \tag{2.5}$$

$$= \operatorname{Res}(f,g) \cdot \prod_{1 \le i < j \le n} (x_i - x_j) \cdot \prod_{1 \le i < j \le k} (y_i - y_j) \cdot \prod_{i=1}^{n} \prod_{j=i}^{k} (y_j - x_i). \tag{2.6}$$

Let $z \in R$ be arbitrary. The scalar product of the vectors

$$\left(\underbrace{0,\ \cdots,\ 0}_{r\text{-times}},\ a_n,\ a_{n-1},\ \cdots,\ a_0,\ 0,\ \cdots,\ 0 \right), \text{ and}$$
$$\left(z^{n+k-1},\ z^{n+k-2},\ \cdots,\ z^0 \right)$$

is $a_n z^{n+k-1-r} + a_{n-1} z^{n+k-2-r} + \ldots + a_0 z^{n+k-n-1-r} = z^{k-1-r} f(z)$. And similarly for the a_i's replaced by the b_i's. Hence,

$$S \cdot V = \begin{pmatrix} y_1^{k-1} f(y_1) & \cdots & y_k^{k-1} f(y_k) & x_1^{k-1} f(x_1) & \cdots & x_n^{k-1} f(x_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ y_1^0 f(y_1) & \cdots & y_k^0 f(y_k) & x_1^0 f(x_1) & \cdots & x_n^0 f(x_n) \\ y_1^{n-1} g(y_1) & \cdots & y_k^{n-1} g(y_k) & x_1^{n-1} g(x_1) & \cdots & x_n^{n-1} g(x_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ y_1^0 g(y_1) & \cdots & y_k^0 g(y_k) & x_1^0 g(x_1) & \cdots & x_n^0 g(x_n) \end{pmatrix}.$$

Since, $f(x_i) = g(y_j) = 0$ for all $i \in \{1, \ldots, n\}$ and $j \in \{1, \ldots, k\}$, it follows that

$$S \cdot V = \begin{pmatrix} y_1^{k-1} f(y_1) & \cdots & y_k^{k-1} f(y_k) & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ y_1^0 f(y_1) & \cdots & y_k^0 f(y_k) & 0 & \cdots & 0 \\ 0 & \cdots & 0 & x_1^{n-1} g(x_1) & \cdots & x_n^{n-1} g(x_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & x_1^0 g(x_1) & \cdots & x_n^0 g(x_n) \end{pmatrix}.$$

Applying the standard rules for the determinant and the formula for calculating the determinant of a Vandermonde-matrix, yields

$$\det(S \cdot V) = \left(\prod_{j=1}^{k} f(y_j) \cdot \det \begin{pmatrix} y_1^{k-1} & \cdots & y_k^{k-1} \\ \vdots & \ldots & \vdots \\ y_1^0 & \cdots & y_k^0 \end{pmatrix} \right) \cdot \left(\prod_{i=1}^{n} g(x_i) \cdot \det \begin{pmatrix} x_1^{n-1} & \cdots & x_n^{n-1} \\ \vdots & \ldots & \vdots \\ x_1^0 & \cdots & x_n^0 \end{pmatrix} \right)$$
$$= \prod_{j=1}^{k} f(y_j) \cdot \prod_{i=1}^{n} g(x_i) \cdot \prod_{1 \le i < j \le k} (y_i - y_j) \cdot \prod_{1 \le i < j \le n} (x_i - x_j). \tag{2.7}$$

[2]If it is not well-known to you, then change this situation! The proof is by induction on the number of variables.

Since R is an integral domain and all factors in the equations (2.5) and (2.7) are non-zero, combining these formulas gives

$$\begin{aligned}
&\operatorname{Res}(f,g)\cdot\prod_{i=1}^{n}\prod_{j=i}^{k}(y_j-x_i)=\prod_{j=1}^{k}f(y_j)\cdot\prod_{i=1}^{n}g(x_i)\\
&=\left(a_n\prod_{i=1}^{n}(y_1-x_i)\right)\cdot\ldots\cdot\left(a_n\prod_{i=1}^{n}(y_k-x_i)\right)\cdot\left(b_k\prod_{j=1}^{k}(x_1-y_j)\right)\cdot\ldots\cdot\left(b_k\prod_{j=1}^{k}(x_n-y_j)\right)\\
&\implies \operatorname{Res}(f,g)=a_n^k b_k^n\cdot\prod_{i=1}^{n}\prod_{j=1}^{k}(x_i-y_j)
\end{aligned}$$

This proves the Theorem. □

Remark 2.1.21. The very same proof applies without changes to the setting, where $f(x)$, $g(x)\in\mathbb{Z}[x]$ and the roots of f and g are pairwise distinct. But using this more general setting, we get this formula also in the case where f and g have a common root. The formula predicts that in this setting the resultant of f and g is zero.

Corollary 2.1.22. *Let R be an integral domain with field of fractions K. Let $f(x)=a_nx^n+\ldots$ and $g(x)=b_kx^k+\ldots$ be polynomials in $R[x]$, with roots $\alpha_1,\ldots,\alpha_n\in\overline{K}$, resp. $\beta_1,\ldots,\beta_k\in\overline{K}$, where $\overline{K}$ is an algebraic closure of K. Then*

(i) $\operatorname{Res}(f,g)=a_n^kb_k^n\prod_{i=1}^{n}\prod_{j=1}^{k}(\alpha_i-\beta_j)\in R$,

(ii) $\operatorname{Res}(f,g)=a_n^k\prod_{i=1}^{n}g(\alpha_i)$,

(iii) $\operatorname{Res}(f,g)=(-1)^{nk}\operatorname{Res}(g,f)$.

Proof. We just plug in the roots $\alpha_1,\ldots\beta_k$ into the polynomial formula from Theorem 2.1.20. Formally:
Consider the polynomial ring $R[x_1,\ldots,x_n,y_1,\ldots,y_k]$ and let φ be the unique ring homomorphism from $R[x_1,\ldots,x_n,y_1,\ldots,y_k]$ to $\overline{K}$, satisfying $\varphi(x_i)=\alpha_i$ for all $i\in\{1,\ldots,n\}$, $\varphi(y_j)=\beta_j$ for all $j\in\{1,\ldots,k\}$, and $\varphi(r)=r$ for all $r\in R$. This gives

$$\operatorname{Res}(f,g)=\varphi(\underbrace{\operatorname{Res}(f,g)}_{\in R})\overset{2.1.20}{=}\varphi(\underbrace{a_n^kb_k^n}_{\in R}\prod_{i=1}^{n}\prod_{j=1}^{k}(x_i-y_j))\overset{\varphi\text{ hom.}}{=}a_n^kb_k^n\prod_{i=1}^{n}\prod_{j=1}^{k}(\alpha_i-\beta_j).$$

Hence part (i) is proven. Part (ii) follows, since $g(\alpha_i)=b_k\prod_{j=1}^{k}(\alpha_i-\beta_j)$, by definition of g. For part (iii), we just have to note that $(\alpha_i-\beta_j)=(-1)(\beta_j-\alpha_i)$. Alternatively, the matrix (2.2) defining $\operatorname{Res}(f,g)$ can be transferred to the matrix defining $\operatorname{Res}(g,f)$ by interchanging rows nk-times. □

We give another application of the resultant.

Corollary 2.1.23. *Let $f(x),g(x)\in\mathbb{Z}[x]$, such that $\alpha\in\mathbb{C}$ is a root of f and $\beta\in\mathbb{C}$ is a root of g. We consider the ring $R=\mathbb{Z}[y]$, where y is a formal variable.*

(i) Consider $f(x),g(y-x)$ as polynomials in $R[x]$. Then $r(y)=\operatorname{Res}(f(x),g(y-x))\in R\setminus\{0\}=\mathbb{Z}[y]\setminus\{0\}$, and $r(\alpha+\beta)=0$.

(ii) Consider $f(x), x^{\deg(g)}g(\frac{y}{x})$ *as polynomials in* $R[x]$*. Then* $r(y) = \mathrm{Res}(f(x), x^{\deg(g)}g(\frac{y}{x})) \in R \setminus \{0\} = \mathbb{Z}[y] \setminus \{0\}$*, and* $r(\alpha \cdot \beta) = 0$*.*

Proof. Since both proofs are essentially the same, we only prove part (i). Let $f(x) = a_n(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$ and $g(x) = b_k(x - \beta_1) \cdot \ldots \cdot (x - \beta_k)$. Then

$$\mathrm{Res}(f(x), g(y - x)) = a_n^k b_k^n \prod_{i=1}^{n} g(y - \alpha_i) \in R \setminus \{0\}.$$

Plugging in $\alpha_j + \beta$ for any $j \in \{1, \ldots, n\}$ and any root β of g, yields a factor $g(\alpha_j + \beta - \alpha_j) = g(\beta) = 0$, proving the claim. □

Remark 2.1.24. Starting with two monic polynomials (leading coefficient equal to 1), guarantees that also the resultants in statements (i) and (ii) are monic. Hence, this reproves (quite effectively) the well-known theorem, that the set of algebraic integers forms a ring.

Lemma 2.1.25. *For all* $\alpha, \beta \in \mathbb{C}$ *the following inequalities hold true:*

$$|\alpha - \beta| \leq 2\max\{|\alpha|, |\beta|\} \leq 2\max\{1, |\alpha|\}\max\{1, |\beta|\}.$$

Proof. The triangular inequality tells us

$$|\alpha - \beta| \leq |\alpha| + |\beta| \leq 2\max\{|\alpha|, |\beta|\}.$$

This proves the first inequality. But obviously

$$\max\{|\alpha|, |\beta|\} \leq \max\{1, |\alpha|, |\beta|, |\alpha\beta|\} = \max\{1, |\alpha|\}\max\{1, |\beta|\},$$

proving the lemma. □

Proposition 2.1.26. *Let* $\alpha, \beta \in \overline{\mathbb{Q}}$ *such that* $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$*,* $k = [\mathbb{Q}(\beta) : \mathbb{Q}]$*, and* α *and* β *do not have the same minimal polynomial. Then*

$$|\alpha - \beta| \geq \frac{1}{2^{dk}M(\alpha)^k M(\beta)^d}.$$

Proof. The minimal polynomial of α is $f(x) = a_d x^d + \ldots \in \mathbb{Z}[x]$ and the minimal polynomial of β is $g(x) = b_k x^k + \ldots \in \mathbb{Z}[x]$ and by assumption $a_d \neq 0 \neq b_k$. Denote the roots of f by $\alpha_1, \ldots, \alpha_d$, and the roots of g by $\beta_1, \ldots, \beta_k$. Since $f(\alpha) = 0 = g(\beta)$ we may and will assume $\alpha = \alpha_1$ and $\beta = \beta_1$. Since $f \neq g$ and both polynomials are irreducible, it follows that $\alpha_i \neq \beta_j$ for all $(i, j) \in \{1, \ldots, d\} \times \{1, \ldots, k\}$. By Corollary 2.1.22, we know that $0 \neq \mathrm{Res}(f, g) \in \mathbb{Z}$. Hence,

$$1 \leq |\mathrm{Res}(f, g)|. \tag{2.8}$$

More precisely, Corollary 2.1.22 tells us

$$\begin{aligned}
|\mathrm{Res}(f,g)| &= \left|a_d^k b_k^d\right| \cdot |\alpha_1-\beta_1| \cdot \prod_{(i,j)\in\{1,\dots,d\}\times\{1,\dots,k\}\setminus\{(1,1)\}} |\alpha_i-\beta_j| \\
&\overset{2.1.25}{\leq} \left|a_d^k b_k^d\right| \cdot |\alpha_1-\beta_1| \cdot \prod_{(i,j)\in\{1,\dots,d\}\times\{1,\dots,k\}\setminus\{(1,1)\}} 2\max\{1,|\alpha_i|\}\max\{1,|\beta_j|\} \\
&\leq \left|a_d^k b_k^d\right| \cdot |\alpha_1-\beta_1| \cdot \prod_{(i,j)\in\{1,\dots,d\}\times\{1,\dots,k\}} 2\max\{1,|\alpha_i|\}\max\{1,|\beta_j|\} \\
&= \left|a_d^k b_k^d\right| \cdot |\alpha_1-\beta_1| \cdot 2^{dk} \prod_{i=1}^{d} \max\{1,|\alpha_i|\}^k \prod_{j=1}^{k} \max\{1,|\beta_j|\}^d \\
&= |\alpha_1-\beta_1|\, 2^{dk} \left(|a_d| \cdot \prod_{i=1}^{d} \max\{1,|\alpha_i|\}\right)^k \cdot \left(|b_k| \cdot \prod_{j=1}^{k} \max\{1,|\beta_j|\}\right)^d \\
&= |\alpha_1-\beta_1|\, 2^{dk} M(\alpha)^k M(\beta)^d.
\end{aligned}$$

Applying (2.8), gives $1 \leq |\alpha_1-\beta_1|\, 2^{dk} M(\alpha)^k M(\beta)^d = |\alpha-\beta|\, 2^{dk} M(\alpha)^k M(\beta)^d$, proving the claim. □

Maybe you have noticed that his is a very familiar statement.

Corollary 2.1.27. *Let $\alpha \in \overline{\mathbb{Q}}$ be of degree $d \geq 2$, and let K be a number field. Then there exists a positive constant $c_K(\alpha) > 0$ such that for all $\beta \in K \setminus \{\alpha\}$ we have*

$$|\alpha-\beta| \geq \frac{c_K(\alpha)}{M(\beta)^d}.$$

Proof. Just let $c_K(\alpha)$ be less than the minimum of the distance between α and any Galois conjugate of α and less than $\frac{1}{2^{dk}M(\alpha)^{[K:\mathbb{Q}]}}$. Then the statement follows immediately from Proposition 2.1.26. □

Remark 2.1.28. This is Liouville's Theorem 1.1.12 for arbitrary number fields! So in this case, the Mahler measure is indeed the correct quantity to measure the quality of an approximation. In particular, Roth's theorem for number fields will be the obvious generalization of (RT3), namely for any number field K it is

$$\forall\, \alpha \in \overline{\mathbb{Q}},\ \forall\, \varepsilon > 0,\ \exists\, c_K(\alpha,\varepsilon) > 0, \text{ such that } |\alpha-\beta| > c_K(\alpha,\varepsilon) \cdot M(\beta)^{-(2+\varepsilon)}, \quad \forall\, \beta \in K\setminus\{\alpha\}. \tag{RT4}$$

In the exercises you will prove that (RT4) is equivalent to the following statement: For any number field K we have

$$\forall\, \alpha \in \overline{\mathbb{Q}},\ \forall\, \varepsilon > 0,\ \text{the set } \left\{\beta \in K \mid\ |\alpha-\beta| < M(\beta)^{-(2+\varepsilon)}\right\} \text{ is finite.} \tag{RT5}$$

Exercises

Exercise 2.1. (a) Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ be arbitrary. Calculate $M(\sqrt[n]{a})$, for any choice of the n-th root.

(b) Prove that $M(\alpha) \geq 2$ for all $\alpha \in \overline{\mathbb{Q}}$ which are not an algebraic unit. Recall, that an algebraic unit is an unit in the ring of algebraic integers.

(c) Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic integer with Galois conjugates $\alpha = \alpha_1, \ldots, \alpha_d$. Assume that none of the quotients α/α_i, $i \in \{2, \ldots, d\}$, is a root of unity. Show that for all $n \in \mathbb{N}$, we have $M(\alpha^n) = M(\alpha)^n$.

Exercise 2.2. Aim is to prove a Theorem of Andrej Schinzel, on the Mahler measure of *totally real* algebraic integers.

(a) Let $x \in (0,1)$ be arbitrary. Prove that $\log(x) + \frac{1}{\sqrt{5}} \log(\frac{1}{x} - x) \leq \log(\frac{2}{1+\sqrt{5}})$.

Hint: Consider the left hand side as a function in x. Take the derivative of this function and use elementary calculus.

(b) Prove that

$$\frac{\max\{1, |x|\}}{|x| \cdot \left|\frac{1}{x} - x\right|^{\frac{1}{\sqrt{5}}}} \geq \frac{1+\sqrt{5}}{2}$$

for all $x \in \mathbb{R} \setminus \{0, \pm 1\}$.

Hint: Use (a) for the case $|x| < 1$. Then replace x by x^{-1}.

(c) Let $f(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_d) \in \mathbb{Z}[x]$ be irreducible, with $d \geq 2$. Prove that

$$\prod_{i=1}^{d} |\alpha_i|^{\frac{1}{2}} \left|\frac{1}{\alpha_i} - \alpha_i\right|^{\frac{1}{2\sqrt{5}}} = |f(0)|^{\frac{1}{2} - \frac{1}{2\sqrt{5}}} \cdot |f(1)f(-1)|^{\frac{1}{2\sqrt{5}}}.$$

Hint: Vieta's formulas.

(d) Let α be an algebraic integer of degree $d \geq 2$, such that all Galois conjugates of α are in $\mathbb{R}$. Prove that $M(\alpha) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{d}{2}}$.

Hint: Combine parts (b) and (c).

(e) Conclude that Lehmers conjecture is true for all totally real numbers, i.e. for all $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$ such that all Galois conjugates of α are real.

Exercise 2.3. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in \mathbb{Z}[x]$, with $f(x) = a_d(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$, for some $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ (so in particular $a_d \neq 0$). The *discriminant* of f is defined as

$$\Delta(f) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Prove that $\Delta(f) = a_n^{-1}(-1)^{\frac{n(n-1)}{2}} \operatorname{Res}(f, f')$, where f' is the derivative of f.

Exercise 2.4. Prove part (ii) in Corollary 2.1.23.

Exercise 2.5. We recall Haramard's determinant inequality from linear algebra: For every $A = (a_{ij}) \in M_n(\mathbb{C})$ we have

$$|\det(A)|^2 \leq \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |a_{ij}|^2 \right).$$

Let $\alpha \in \overline{\mathbb{Q}}$ be of degree d, with minimal polynomial $f \in \mathbb{Z}[x]$. Use Hadamard's inequality, to prove $|\Delta(f)| \leq d^d M(\alpha)^{2d-2}$.

Exercise 2.6. Prove that (RT4) and (RT5) are equivalent.

Exercise 2.7. By Northcott's theorem the set $M_d = \{M(\alpha) | [\mathbb{Q}(\alpha) : \mathbb{Q}] = d\}$ is discrete for all $d \in \mathbb{N}$.

(a) Find the two smallest values in $M_2 \setminus \{1\}$.

(b) Find the smallest value in $M_3 \setminus \{1\}$.

2.2 Recap on Valuation Theory

I assume that you have basic knowledge of valuation theory. The material provided by the course *algebraic number theory* by Prof. Kohlhaase last term, should be sufficient. To guarantee that all of us stand more or less on the same ground, I will recall the most important results and definitions. The proofs are skipped or sketched. In addition to an lecture on algebraic number theory, everything can be found in the books [10] and [6].

2.2.1 Absolute Values, Ramification, Inertia

First of all, recall that all number fields are contained in a fixed algebraic closure $\overline{\mathbb{Q}} \subseteq \mathbb{C}$. Given any complex number z (so in particular any element in $\overline{\mathbb{Q}}$), the complex conjugate of z is denoted by $\overline{z}$.

Definition 2.2.1. Let K be a field. An *absolute value* on K is a function $|.| : K \to \mathbb{R}$ satisfying

(i) $|a| \geq 0$ and $|a| = 0 \iff a = 0$,

(ii) $|a \cdot b| = |a| \cdot |b|$, and

(iii) $|a + b| \leq |a| + |b|$,

for all $a, b \in K$. If $|.|$ satisfies the *ultrametric inequality*

(iii') $|a + b| \leq \max\{|a|, |b|\}$,

then $|.|$ is called *non-archimedean*. Otherwise, it is called *archimedean*. The *trivial absolute value* $|.|_0$ is given by $|0|_0 = 0$ and $|a|_0 = 1$ for all $a \in K^*$.

If $|.|$ is non-archimedean, then $|a| \neq |b|$ implies $|a + b| = \max\{|a|, |b|\}$: Assume $|a| > |b|$, then surely $|a + b| \leq \max\{|a|, |b|\} = |a|$. On the other hand, we have $|a| = |a + b - b| \leq \max\{|a + b|, |b|\}$. Since $|a| > |b|$, it follows $|a| \leq |a + b|$, proving the claim.
It is easy to check that if $|.|$ is an absolute value on the field K, then so is $|.|^\varepsilon$ for any $\epsilon \in [0, 1]$.

Definition 2.2.2. Let K be a field. Two absolute values $|.|_1$ and $|.|_2$ on K are *equivalent*, if and only if there is an $\varepsilon > 0$ such that $|a|_1 = |a|_2^\varepsilon$ for all $a \in K$.

Equivalently, one could say that two absolute values on K are equivalent if and only if they induce the same topology on K.

Example 2.2.3. On $\mathbb{Q}$ we have the usual (archimedean) absolute value $|\alpha|_\infty = \max\{\alpha, -\alpha\}$. Let p be a prime number. Every $\alpha \in \mathbb{Q}^*$ can be written as $\alpha = p^{v_p(\alpha)} \cdot \frac{a}{b}$ with $v_p(\alpha), a, b \in \mathbb{Z}$, and $p \nmid a \cdot b$. Obviously, this $v_p(\alpha)$ is uniquely determined. Now, the *p-adic absolute value* of $\alpha \in \mathbb{Q}^*$ is given by $|\alpha|_p = p^{-v_p(\alpha)}$ (and of course $|0|_p = 0$).

Lemma 2.2.4. *Let $\mathbb{P}$ be the set of all primes. Then $\prod_{p \in \mathbb{P} \cup \{\infty\}} |\alpha|_p = 1$ for all $\alpha \in \mathbb{Q}^*$.*

Proof. Write $\alpha = \frac{a}{b}$ with coprime $a, b \in \mathbb{Z}$. Since it clearly suffices to check the claim for positive numbers, we assume $a, b \in \mathbb{N}$. Then for all $p \in \mathbb{P}$ we have

$$|\alpha|_p = \begin{cases} p^{-v_p(a)} & \text{if } p \mid a \\ p^{v_p(b)} & \text{if } p \mid b \\ 1 & \text{else.} \end{cases}$$

Hence $\prod_{p \in \mathbb{P}} |\alpha|_p = \frac{b}{a}$, proving the lemma. □

Theorem 2.2.5. *Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to $|.|_\infty$ or to $|.|_p$ for some prime number p.*

We set

$$M_{\mathbb{Q}} = \{|.|_p \, | p \in \mathbb{P}\} \cup \{|.|_\infty\}. \tag{2.9}$$

Now we do the same for an arbitrary number field K. There are precisely $[K : \mathbb{Q}]$ embeddings of K into $\mathbb{C}$ (or equivalently $\overline{\mathbb{Q}}$). Here an embedding is just a ring-homomorphism, which is necessarily injective, since K is a field, and necessarily every element in $\mathbb{Q}$ is fixed, since $1 \mapsto 1$ and it is a ring-homomorphism. We denote the set of embeddings of K by $\mathrm{Hom}_{\mathbb{Q}}(K/\mathbb{C})$.
Let $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ and let $|.|$ be the usual absolute value on $\mathbb{C}$. This is: For $z = a + b \cdot i \in \mathbb{C}$, we have $|z| = \sqrt{a^2 + b^2} = \sqrt{z \cdot \overline{z}}$.
Then (obviously) $|\sigma(.)|$ is an archimedean absolute value on K. Given any $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$, the map

$$\overline{\sigma} : K \longrightarrow \mathbb{C} \quad ; \quad \alpha \mapsto \overline{\sigma(\alpha)}$$

is also in $\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$. We have $\sigma = \overline{\sigma}$ if and only if all values of σ are real. In this case σ is called a *real embedding*, otherwise it is called a *complex embedding*.

Theorem 2.2.6. *Let $\sigma_1, \ldots, \sigma_r, \sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}$ be all embeddings of the number field K. (Note that this implies $[K : \mathbb{Q}] = r + 2s$.) Then there are precisely $r + s$ non-equivalent archimedean absolute values on K, namely*

$$|.|_{\sigma_i} = |\sigma_i(.)| \quad \text{for } i \in \{1, \ldots, r+s\}. \tag{2.10}$$

Remark 2.2.7. Note that this differs from Prof. Kohlhaase's notation. This is due to the fact that $\|.\|_\sigma = \left|\sigma(.) \cdot \overline{\sigma(.)}\right|$ is in general NOT an absolute value!

The non-archimedean absolute values of K are still missing. In the case $K = \mathbb{Q}$ we used the unique prime decomposition in $\mathbb{Z}$. Now $\mathbb{Z}$ is just the ring of (algebraic) integers in $\mathbb{Q}$. Denote with $\mathcal{O}_K$ the ring of (algebraic) integers in K. Then there is not necessarily an unique prime decomposition in $\mathcal{O}_K$, but there is a unique prime ideal decomposition! So we can mimic the construction of the p-adic absolute values, with prime ideals instead of prime elements.
Let $\mathcal{P}$ be a prime ideal in $\mathcal{O}_K$ and let $\alpha \in K^*$ be arbitrary. Write $\alpha = \frac{\alpha_1}{\alpha_2}$ with $\alpha_1, \alpha_2 \in \mathcal{O}_K$ (which is always possible, since K is the field of fractions of $\mathcal{O}_K$). There are non-negative

integers $v_{\mathcal{P}}(\alpha_1), v_{\mathcal{P}}(\alpha_2)$ such that $\alpha_i \in \mathcal{P}^{v_{\mathcal{P}}(\alpha_i)}$ and $\alpha_i \notin \mathcal{P}^{v_{\mathcal{P}}(\alpha_i)+1}$ for $i \in \{1,2\}$. Set $v_{\mathcal{P}}(\alpha) = v_{\mathcal{P}}(\alpha_1) - v_{\mathcal{P}}(\alpha_2)$, then we define

$$\|\alpha\|_{\mathcal{P}} = N(\mathcal{P})^{-v_{\mathcal{P}}(\alpha)},$$

where $N(\mathcal{P}) = |\mathcal{O}_K/\mathcal{P}|$ is the *norm of* $\mathcal{P}$. Using fractional ideals, we have a *unique prime ideal decomposition* $\alpha\mathcal{O}_K = \prod_{\mathcal{P}} \mathcal{P}^{v_{\mathcal{P}}(\alpha)}$, where the product runs over all prime ideals in $\mathcal{O}_K$.
Since $\mathcal{P}$ is a prime ideal, and $\mathcal{O}_K$ is a Dedekind domain, it is actually a maximal ideal and $\mathcal{O}_K/\mathcal{P}$ is a field of characteristic p for a (necessarily unique) prime number $p \in \mathcal{P}$. Hence, $N(\mathcal{P}) = p^{f_{\mathcal{P}|p}}$ for some integer $f_{\mathcal{P}|p} \in \mathbb{N}$ which we call the *inertia degree* of $\mathcal{P}$ over p. In particular,

$$\|\alpha\|_{\mathcal{P}} = N(\mathcal{P})^{-v_{\mathcal{P}}(\alpha)} = p^{-f_{\mathcal{P}|p} v_{\mathcal{P}}(\alpha)}.$$

Let us define the inertia degree in a slightly more general setting.

Definition 2.2.8. Let L/K be an extension of number fields. Moreover, let $\mathcal{P}$ be a prime ideal in $\mathcal{O}_K \subseteq \mathcal{O}_L$ and $\mathfrak{P} \supseteq \mathcal{P}$ be a prime ideal in $\mathcal{O}_L$. Then we say that $\mathfrak{P}$ *lies above* $\mathcal{P}$ and the inertia degree of $\mathfrak{P}$ over $\mathcal{P}$ is given by $f_{\mathfrak{P}|\mathcal{P}} = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathcal{P}]$.

Note that this is well-defined and in the case $K = \mathbb{Q}$ and $\mathcal{P} = p\mathbb{Z}$, we indeed recover the first definition of the inertia degree.

Theorem 2.2.9. *For any prime ideal $\mathcal{P}$ in $\mathcal{O}_K$, the function $\|.\|_{\mathcal{P}}$ (with the convention $\|0\|_{\mathcal{P}} = 0$) is a non-archimedean absolute value on K. Moreover, whenever $\|.\|$ is a non-trivial non-archimedean absolute value on K, the set $\mathcal{P} = \{\alpha \in K | \, \|\alpha\| < 1\} \cap \mathcal{O}_K$ is a prime ideal in $\mathcal{O}_K$, and $\|.\|$ is equivalent to $\|.\|_{\mathcal{P}}$.*

Let p be a prime number. Since $p\mathcal{O}_K$ has a unique prime ideal decomposition, there are prime ideals $\mathcal{P}_1, \ldots, \mathcal{P}_n$ in $\mathcal{O}_K$, such that $p\mathcal{O}_K = \mathcal{P}_1^{e_{\mathcal{P}_1|p}} \cdot \ldots \cdot \mathcal{P}_n^{e_{\mathcal{P}_n|p}}$, with $e_{\mathcal{P}_i|p} \geq 1$ for all $i \in \{1, \ldots, n\}$. (In the notation above it is $e_{\mathcal{P}_i|p} = v_{\mathcal{P}_i}(p)$.) This means, that the $\mathcal{P}_i$'s are precisely the prime ideals in $\mathcal{O}_K$ containing p. The integer $e_{\mathcal{P}_i|p}$ is called *ramification index of $\mathcal{P}_i$ over p*. Now, for any $i \in \{1, \ldots, n\}$ it is

$$\|p\|_{\mathcal{P}_i} = p^{-f_{\mathcal{P}_i|p} e_{\mathcal{P}_i|p}}.$$

Since $|p|_p = p^{-1}$ for the usual p-adic absolute value, the absolute value of p depends on the chosen ground field K and the chosen prime ideal above p. This is very unpleasant!
Before we proceed let us again define the ramification index in a slightly more general setting.

Definition 2.2.10. Let L/K be an extension of number fields, and let $\mathcal{P}$ be a prime ideal in $\mathcal{O}_K$. Then by the unique prime ideal decomposition, there are finitely many prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ in $\mathcal{O}_L$ such that

$$\mathcal{P}\mathcal{O}_L = \prod_{i=1}^{n} \mathfrak{P}_i^{e_{\mathfrak{P}_i|\mathcal{P}}},$$

for positive integers $e_{\mathfrak{P}_1|\mathcal{P}}, \ldots, e_{\mathfrak{P}_n|\mathcal{P}}$. The prime ideals $\mathfrak{P}_i$ are precisely the prime ideals above $\mathcal{P}$, and $e_{\mathfrak{P}_i|\mathcal{P}}$ is the *ramification index* of $\mathfrak{P}_i$ over $\mathcal{P}$.

Lemma 2.2.11. *Let $F/L/K$ be extensions of number fields. Moreover, let $\mathfrak{p}$, $\mathfrak{P}$, $\mathcal{P}$, be prime ideals in $\mathcal{O}_F$, $\mathcal{O}_L$, resp. $\mathcal{O}_K$, such that $\mathcal{P} \subseteq \mathfrak{P} \subseteq \mathfrak{p}$. Then*

(i) $\mathcal{P} = \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p} \cap \mathcal{O}_K$ and $\mathfrak{P} = \mathfrak{p} \cap \mathcal{O}_L$.

(ii) $e_{\mathfrak{p}|\mathfrak{P}} \cdot e_{\mathfrak{P}|\mathcal{P}} = e_{\mathfrak{p}|\mathcal{P}}$.

(iii) $f_{\mathfrak{p}|\mathfrak{P}} \cdot f_{\mathfrak{P}|\mathcal{P}} = f_{\mathfrak{p}|\mathcal{P}}$.

(iv) If L/K is a Galois extension, and $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are two prime ideals in $\mathcal{O}_L$ lying above $\mathcal{P}$, then $e_{\mathfrak{P}_1|\mathcal{P}} = e_{\mathfrak{P}_2|\mathcal{P}}$, and $f_{\mathfrak{P}_1|\mathcal{P}} = f_{\mathfrak{P}_2|\mathcal{P}}$.

We resume the study of non-archimedean absolute values on a number field K. We define for any prime ideal $\mathcal{P}$ in $\mathcal{O}_K$

$$|.|_{\mathcal{P}} = \|.\|_{\mathcal{P}}^{\frac{1}{f_{\mathcal{P}|p}e_{\mathcal{P}|p}}} = p^{-\frac{v_{\mathcal{P}}(.)f_{\mathcal{P}|p}}{f_{\mathcal{P}|p}e_{\mathcal{P}|p}}} = p^{-\frac{v_{\mathcal{P}}(.)}{e_{\mathcal{P}|p}}}, \tag{2.11}$$

where p is the unique prime number in $\mathcal{P}$. Since $\frac{1}{f_{\mathcal{P}|p}e_{\mathcal{P}|p}} \leq 1$, we know that $|.|_{\mathcal{P}}$ is again a non-archimedean absolute value. The benefit of this normalization is the following

Proposition 2.2.12. *Let L/K be an extension of number fields, and let $\mathfrak{P}$ and $\mathcal{P}$ be prime ideals in $\mathcal{O}_L$, resp. $\mathcal{O}_K$, such that $\mathfrak{P}$ lies above $\mathcal{P}$. Then $|.|_{\mathfrak{P}}$ restricted to K is equal to $|.|_{\mathcal{P}}$.*

Proof. Let $\alpha \in K^*$ be arbitrary. Since $\mathcal{P}$ appears exactly $v_{\mathcal{P}}(\alpha)$-times in the prime ideal decomposition of $\alpha\mathcal{O}_K$, and $\mathfrak{P}$ appears precisely $e_{\mathfrak{P}|\mathcal{P}}$-times in the prime ideal decomposition of $\mathcal{P}\mathcal{O}_L$, the prime ideal $\mathfrak{P}$ appear precisely $v_{\mathcal{P}}(\alpha)e_{\mathfrak{P}|\mathcal{P}}$-times in the prime ideal decomposition of $\alpha\mathcal{O}_L$. This just means that we have

$$v_{\mathfrak{P}}(\alpha) = v_{\mathcal{P}}(\alpha)e_{\mathfrak{P}|\mathcal{P}}. \tag{2.12}$$

That is already the main observation, since

$$|\alpha|_{\mathfrak{P}} = p^{-v_{\mathfrak{P}}(\alpha)/e_{\mathfrak{P}|p}} \overset{(2.12)}{=} p^{-v_{\mathcal{P}}(\alpha)e_{\mathfrak{P}|\mathcal{P}}/e_{\mathfrak{P}|p}} \overset{2.2.11}{=} p^{-v_{\mathcal{P}}(\alpha)e_{\mathfrak{P}|\mathcal{P}}/e_{\mathfrak{P}|\mathcal{P}}e_{\mathcal{P}|p}} = p^{-v_{\mathcal{P}}(\alpha)/e_{\mathcal{P}|p}} = |\alpha|_{\mathcal{P}}.$$

□

Let us summarize what we have done so far. We have classified all absolute values on the number field K. Let again $\sigma_1, \ldots, \sigma_r$ be the real embeddings of K, and $\sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots \sigma_{r+s}, \overline{\sigma_{r+s}}$ be the complex embeddings of K. Then the following is a full list of pairwise non-equivalent absolute values on K:

(i) the trivial one,

(ii) (the archimedean ones) $|.|_{\sigma_i}$, with $i \in \{1, \ldots, r+s\}$, normalized as in (2.10) and

(iii) (the non-archimedean ones) $|.|_{\mathcal{P}}$, with $\mathcal{P}$ a prime ideal in $\mathcal{O}_K$, normalized as in (2.11).

We set

$$M_K = \{|.|_{\sigma_i} \,|i \in \{1, \ldots, r+s\}\} \cup \{|.|_{\mathcal{P}} \,|\mathcal{P} \text{ prime ideal in } \mathcal{O}_K\}. \tag{2.13}$$

By (maybe heavy) abuse of notation, we will often identify the absolute value $|.|_v \in M_K$ with its index v.

Definition 2.2.13. Let L/K an extension of number fields, and let $v \in M_K$ and $w \in M_L$. If w restricted to K is equal to v, then we denote this by $w \mid v$ and say that w is an extension of v to L. If w is not an extension of v we write $w \nmid v$. In particular, v is archimedean if and only if $v \mid \infty$, and v is non-archimedean if and only if there is a prime number p such that $v \mid p$.
If v and w are non-archimedean, and they correspond to $\mathcal{P}$ and $\mathfrak{P}$ resp., then we define the ramification index $e_{w|v} = e_{\mathfrak{P}|\mathcal{P}}$ and the inertia degree $f_{w|v} = f_{\mathfrak{P}|\mathcal{P}}$. If v and w are archimedean, corresponding to the embeddings σ, and τ, then we define the ramification index

$$e_{w|v} = \begin{cases} 1 & \text{if } \sigma,\ \tau \text{ are both real or both complex} \\ 2 & \text{if } \sigma \text{ is real and } \tau \text{ is complex,} \end{cases}$$

and the inertia degree $f_{w|v} = 1$ in all cases. Note that $w \mid v$ implies that $\tau|_K = \sigma$, hence it is not possible that τ is real and σ is complex.
If $v \mid p$ for some $p \in M_{\mathbb{Q}}$, then we drop the dependence on p and say that $e_v = e_{v|p}$ is the ramification index of v, and $f_v = f_{v|p}$ is the inertia degree of v.

Theorem 2.2.14. *Let L/K be an extension of number fields. For all $v \in M_K$ we have*

$$\sum_{\substack{w \in M_L \\ w|v}} e_{w|v} \cdot f_{w|v} = [L : K].$$

Proof. Let σ be an embedding of K corresponding to the archimedean absolute value $v \in M_K$. By Galois theory, there are precisely $[L : K]$ embeddings of τ of L, such that $\tau|_K = \sigma$. If r of these embeddings are real and $2s$ of these embeddings are complex, then there are $r + s$ extensions of v to L. By definition r of these have ramification index 1 and s of these have ramification index 2. Hence,

$$\sum_{w|v} e_{w|v} f_{w|v} = \sum_{w|v} e_{w|v} = r + 2s = [L : K].$$

If v is non-archimedean, then this result was proven in Kohlhaase's course last term. By the multiplicativity of the ramification index, the inertia degree and the degree of a field extension, it suffices to prove this result in the case, where $K = \mathbb{Q}$, and $v = p$ is a prime number. The idea of the proof was to use the Chinese remainder theorem

$$\mathcal{O}_L/p\mathcal{O}_L \cong \prod_{i=1}^{n} \mathcal{O}_L/\left(\mathcal{P}_i^{e_{\mathcal{P}_i|p}}\right),$$

where $p\mathcal{O}_L = \mathcal{P}_1^{e_{\mathcal{P}_i|p}} \cdot \ldots \cdot \mathcal{P}_n^{e_{\mathcal{P}_i|p}}$ is the prime ideal decomposition of $p\mathcal{O}_L$. This isomorphism is in particular an isomorphism of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$-vector spaces. The claimed statement follows from comparing the dimensions. One proves that the dimension of $\mathcal{O}_L/p\mathcal{O}_L$ is $[L : \mathbb{Q}]$ (one has to do something for this), and that the dimension of $\mathcal{O}_L/\left(\mathcal{P}_i^{e_{\mathcal{P}_i|p}}\right)$ is $e_{\mathcal{P}_i|p} f_{\mathcal{P}_i|p}$ for all $i \in \{1, \ldots, n\}$ (this is quite easy). It then follows

$$[L : \mathbb{Q}] = \sum_{i=1}^{n} e_{\mathcal{P}_i|p} f_{\mathcal{P}_i|p} = \sum_{\substack{v \in M_L \\ v|p}} e_v \cdot f_v,$$

as claimed. □

Corollary 2.2.15. *If $K/\mathbb{Q}$ is a Galois extension, $p \in M_{\mathbb{Q}}$, and n the number of extensions of p to K, then $[K:\mathbb{Q}] = n \cdot e_v \cdot f_v$, for any $v \in M_K$ extending p.*

Recall that the *norm of an element* $\alpha \in K$ is given by $N_{K/\mathbb{Q}}(\alpha) = \prod_{\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K/\mathbb{C})} \sigma(\alpha)$, and that (non-trivially) $\left|N_{K/\mathbb{Q}}(\alpha)\right| = \prod_{\mathcal{P}} N(\mathcal{P})^{v_{\mathcal{P}}(\alpha)}$. This implies the product formula

Theorem 2.2.16. *Let K be a number field, then for all $\alpha \in K^*$ we have*

$$\prod_{v \in M_K} |\alpha|_v^{e_v f_v} = 1.$$

Definition 2.2.17. Let K be a number field. Set $M_K^{\mathrm{fin}} = \{v \in M_K | v \nmid \infty\}$, and let $S \subseteq M_K^{\mathrm{fin}}$ be a finite subset. An $\alpha \in K$ is called an *S-integer* if $|\alpha|_v \leq 1$ for all $v \in M_K^{\mathrm{fin}} \setminus S$. The set of all S-integers is denoted by $\mathcal{O}_{K,S}$.

Proposition 2.2.18. *Let K and S be as above, then $\mathcal{O}_{K,S}$ is a ring, and $\mathcal{O}_{K,\emptyset} = \mathcal{O}_K$.*

Proof. If $\alpha, \beta \in \mathcal{O}_S$ and $v \in M_K^{\mathrm{fin}}$ is arbitrary, then $|\alpha \cdot \beta|_v = |\alpha|_v \cdot |\beta|_v \leq 1$ and $|\alpha + \beta|_v \leq \max\{|\alpha|_v, |\beta|_v\} \leq 1$. Hence, $\alpha \cdot \beta \in \mathcal{O}_{K,S}$ and $\alpha + \beta \in \mathcal{O}_{K,S}$, which proves the first statement. The second statement follows directly from the definition of the absolute value $|.|_v$. □

2.2.2 Completions

Let K be a field with absolute value $|.|$. Then there is a "smallest field" F in which all Cauchy sequences of elements in K converge. This field is called the completion of K with respect to $|.|$. If $|.|$ is archimedean, then the completion is either $\mathbb{R}$ or $\mathbb{C}$. The completion of $\mathbb{Q}$ with respect to the p-adic absolute value $|.|_p$ is the field of p-adic numbers $\mathbb{Q}_p$.
If K is a number field and $v \in M_K$, then the completion of K with respect to v is denoted K_v. The absolute value v extends uniquely to an absolute value on K_v. This is: if $\alpha \in K_v$ then there exists an infinite sequence $\alpha_1, \alpha_2, \ldots \in K$ such that $\alpha = \lim_{i \to \infty} \alpha_i$. Hence, we define $|\alpha|_v = \lim_{i \to \infty} |\alpha_i|_v$. The field K_v is *complete* with respect to this absolute value; i.e. every Cauchy sequence (with respect to v) of elements in K_v converges in K_v.
In the following, we always let K be a number field, and $v \in M_K$ be non-archimedean.

Lemma 2.2.19. *Let F/K_v be a finite extension. Then there is precisely one absolute value ν on F extending v. It is given by $|\alpha|_\nu = \left|N_{F/K_v}(\alpha)\right|_v^{1/[F:K_v]}$. Here $N_{F/K_v}(\alpha)$ is the norm of α; i.e. the product of all $\sigma(\alpha)$, where σ runs through all K_v-embeddings of F into $\overline{K_v}$.*

Lemma 2.2.20. *For every $\alpha \in K_v$, there is a $\beta \in K$ such that $|\alpha|_v = |\beta|_v$.*

Proof. Let $\alpha = \lim_{n \to \infty} \alpha_n$, with $\alpha_n \in K$. Then $|\alpha_n|_v \longrightarrow |\alpha|_v$. But by definition we have

$$|\alpha_n|_v = \frac{1}{p^{\frac{a}{e_v}}} \quad \text{for some } a \in \mathbb{Z}.$$

The set $p^{\mathbb{Z}/e_v} := \{p^{\frac{a}{e_v}} | a \in \mathbb{Z}\} = \{\frac{1}{p^{\frac{a}{e_v}}} | a \in \mathbb{Z}\}$ is discrete, and hence, $|\alpha_n|_v \longrightarrow |\alpha|_v$ either means that $|\alpha|_v = 0$ or $|\alpha|_v = |\alpha_n|_v$ for all large enough n. □

If F is a field with absolute value ν, then we define the set $|F|_\nu = \{|a|_\nu | a \in F^*\}$. This is obviously a group under multiplication. Now we can rephrase the preceding lemma as $|K|_v = |K_v|_v$.

Definition 2.2.21. Let K be a number field with non archimedean valuation $v \in M_K$. Then $\mathcal{O}_v = \{\alpha \in K_v | \, |\alpha|_v \leq 1\}$ is the *ring of v-adic integers.*

Using the ultrametric inequality, it is indeed obvious that $\mathcal{O}_v$ is a ring.

Lemma 2.2.22. *Let $K, v, \mathcal{O}_v$ be as above. Then $\mathcal{O}_v$ is a local ring, with unique prime ideal $\mathcal{M}_v = \{\alpha \in K_v | \, |\alpha|_v < 1\}$. Moreover, $\mathcal{O}_v$ is a principle ideal domain. Denote by p the unique prime number such that $v \mid p$. An element $\pi_v \in K_v$ is a generator of $\mathcal{M}_v$ if and only if $|\pi_v|_v = p^{-1/e_v}$. Such an element is called* uniformizer in K_v.

Proof. Note that π_v is just any element in K_v with largest possible absolute value less than one. If $\alpha \in \mathcal{M}_v$, then $|\alpha|_v < 1$, and hence $|\alpha|_v = p^{-a/e_v} = |\pi_v|_v^a$, for some $a \in \mathbb{N}$. Then, $\left|\pi_v^{a-1} \frac{\alpha}{\pi_v^a}\right|_v \leq 1$, and $\alpha = \pi_v \cdot \pi_v^{a-1} \frac{\alpha}{\pi_v^a} \in \pi_v \cdot \mathcal{O}_v$. □

Lemma 2.2.23. *Let L/K be an extension of number fields and let $w \in M_L$, such that $w \mid v$. Then*

(i) $K_v \subseteq L_w$, and

(ii) $(|L_w|_w : |K_v|_v) = (|L|_w : |K|_v) = e_{w|v}$.

Proof. Since w is an extension of v, every Cauchy sequence of elements in K with respect to w (which is equal to v on K) converges in K_v. This proves part (i). This implies that $|K_v|_v$ is indeed a subgroup of $|L_w|_w$. The first equality in (ii) follows immediately from Lemma 2.2.20. Since $|L|_w = p^{\mathbb{Z}/e_w}$ and $|K|_v = p^{\mathbb{Z}/e_v}$, for the unique prime number satisfying $v \mid p$, we know that the group index $(|L|_w : |K|_v)$ is equal to $\frac{e_w}{e_v} \overset{2.2.11}{=} e_{w|v}$. □

Proposition 2.2.24. *Let L/K be an extension of number fields, and let $w \in M_L$ be such that $w \mid v$. Then $\mathcal{O}_v$ is the completion of $\mathcal{O}_K$ with respect to v, and $\mathcal{O}_w$ is the integral closure of $\mathcal{O}_v$ in L_w.*

Proof. We only sketch the proof of the second statement. Let $\alpha \in L_w$ be integral over $\mathcal{O}_v$. This means that there are $a_0, \ldots, a_{n-1} \in \mathcal{O}_v$ such that

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

This implies

$$|\alpha|_w^n = \left|a_{n-1}\alpha^{n-1} + \ldots + a_0\right|_w \leq \max_{0 \leq i \leq n-1} \{\left|a_i \alpha^i\right|_w\} \leq \max_{0 \leq i \leq n-1} \left|\alpha^i\right|_w,$$

where the last inequality follows, since $|a_i|_w = |a_i|_v \leq 1$ for all $i \in \{0, \ldots, n-1\}$. It follows $|\alpha|_w \leq 1$, and hence $\alpha \in \mathcal{O}_w$.
Now assume that $\alpha \in \mathcal{O}_w$, or equivalently $|\alpha|_w \leq 1$. Let F be the Galois closure of L_w over K_v. By Lemma 2.2.19 there is a unique absolute value ν on F extending w. It follows that $|\sigma(\alpha)|_\nu = |\alpha|_\nu = |\alpha|_w \leq 1$ for all $\sigma \in \mathrm{Gal}(F/K_v)$. Galois theory tells us that

$$\prod_{\sigma \in \mathrm{Gal}(F/K_v)} (x - \sigma(\alpha)) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in K_v[x].$$

Since $|\sigma(\alpha)|_\nu \leq 1$ for all σ, the ultrametric inequality (together with Vieta's formulas 2.1.5) predicts that also $|a_i|_\nu = |a_i|_v \leq 1$ for all $i \in \{0, \ldots, n-1\}$. Hence α is integral over $\mathcal{O}_v$. □

Proposition 2.2.25. *Let $\mathcal{P}$ be the prime ideal in $\mathcal{O}_K$ corresponding to v. Then for all $n \in \mathbb{N}$ we have $\mathcal{O}_K/\mathcal{P}^n \cong \mathcal{O}_v/\mathcal{M}_v^n$.*

Theorem 2.2.26. *Let L/K be an extension of number fields, and let $w \in M_L$ be such that $w \mid v$. Then the* local degree *is $d_{w|v} = [L_w : K_v] = e_{w|v} \cdot f_{w|v}$. In case that $K = \mathbb{Q}$, we simply write d_w for $d_{w|v}$. This is also true if $v \mid \infty$.*

Proof. The proof in the non-archimedean case was done in the number theory course. The archimedean case is true by the definition of e_w and f_w: It is $L_w = \mathbb{R}$ if w corresponds to a real embedding, and $L_w = \mathbb{C}$ if w corresponds to a complex embedding. Moreover $f_w = 1$ in all archimedean cases. Since $\mathbb{Q}_\infty = \mathbb{R}$, we have $d_w = 1 = e_w$ if w corresponds to a real embedding, and $d_w = 2 = e_w$ if w corresponds to a complex embedding. □

Exercises

Exercise 2.8. Let K be a number field, and let p be a prime number. Moreover, we fix a $v \in M_K$ such that $v \mid p$. Prove that for all $\alpha \in \mathcal{O}_v$, with $\alpha \neq \alpha^{p^{f_v}}$, we have $\left|\alpha - \alpha^{p^{f_v}}\right|_v \leq \frac{1}{p^{1/e_v}}$.

2.3 The Weil-height (finally)

All absolute values on a number field will be normalized as in (2.10) and (2.11).

Notation 2.3.1. Let K be a field with absolute value $|.|_\nu$ and let $K[x_1, \ldots, x_n]$ be the polynomial ring over K in n variables. For $\underline{d} = (d_1, \ldots, d_n) \in \mathbb{Z}^n$ define $\underline{x}^{\underline{d}} = x_1^{d_1} \cdot \ldots \cdot x_n^{d_n}$. Any $f \in K[x_1, \ldots, x_n]$ can be written as $f = \sum_{\underline{d} \in \mathbb{N}_0^n} a_{\underline{d}} \underline{x}^{\underline{d}}$, with $a_{\underline{d}} = 0$ for all but finitely many $\underline{d} \in \mathbb{N}_0^n$. Then we set

$$|f|_v = \left| \sum_{\underline{d} \in \mathbb{N}_0^n} a_{\underline{d}} \underline{x}^{\underline{d}} \right|_v = \max_{\underline{d} \in \mathbb{N}_0^n} |a_{\underline{d}}|_v .$$

Lemma 2.3.2 (Gauß-Lemma)**.** *Let K be a number field, and let $v \in M_K$ be non-archimedean. Then $|f \cdot g|_v = |f|_v \cdot |g|_v$ for all $f, g \in K_v[x_1, \ldots, x_n]$.*

Proof. If $f = 0$ or $g = 0$, then surely $|f \cdot g|_v = 0 = |f|_v \cdot |g|_v$. So we assume from now on, that $f \cdot g \neq 0$. For all $\alpha \in K_v$, the definition of $|f|_v$ implies $|\alpha \cdot f|_v = |\alpha|_v \cdot |f|_v$.
Assume first that $|f|_v = 1 = |g|_v$. This means that the absolute value of each coefficient of f and g is ≤ 1, so we have $f, g \in \mathcal{O}_v[x_1, \ldots, x_n]$. Since $\mathcal{O}_v$ is a ring, we know $f \cdot g \in \mathcal{O}_v[x_1, \ldots, x_n]$, which implies $|f \cdot g|_v \leq 1$.
We apply the canonical projection $\pi : \mathcal{O}_v[x_1, \ldots, x_n] \longrightarrow \mathcal{O}_v/\mathcal{M}_v[x_1, \ldots, x_n]$. Since at least one of the coefficients of f and one of the coefficients of g has absolute value $= 1$, this coefficient in not in $\mathcal{M}_v$. Hence $\pi(f) \neq 0 \neq \pi(g)$. Since $\mathcal{O}_v/\mathcal{M}_v$ is a field, it follows $\pi(f \cdot g) = \pi(f) \cdot \pi(g) \neq 0$. But this means that at least one of the coefficients of $f \cdot g$ does not lie in $\mathcal{M}_v$. Hence, it must be $|f \cdot g|_v = 1$.
For arbitrary $f, g \in K_v[x_1, \ldots, x_n] \setminus \{0\}$, we choose $\alpha, \beta \in K_v$ such that $|\alpha \cdot f|_v = 1 = |\beta \cdot g|_v$. (For instance this works if α is the inverse of the maximal coefficient of f). Then, by the special case studied above,

$$|\alpha \cdot \beta|_v \cdot |f \cdot g|_v = |\alpha \cdot f \cdot \beta \cdot g|_v = |\alpha \cdot f|_v \cdot |\beta \cdot g|_v = |\alpha \cdot \beta|_v \cdot |f|_v \cdot |g|_v .$$

This proves the claim. □

Remark 2.3.3. Just for completeness, we will give the proof of the well-known Lemma 2.1.10. The statement was: A polynomial $f \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$, if and only if f is irreducible in $\mathbb{Q}[x]$ and the gcd of its coefficients is equal to one.
The assumption on the gcd just guarantees that f does not have a factor in $\mathbb{Z}$. Hence, if the gcd is 1 and f is irreducible in $\mathbb{Q}[x]$, it is surely irreducible in $\mathbb{Z}[x]$.
Now, let f be irreducible in $\mathbb{Z}[x]$. Then again the gcd is 1. Assume that there are $g, h \in \mathbb{Q}[x]$ such that $f = g \cdot h$. Since $|f|_p \leq 1$ for all primes p, and at least one coefficient is not divisible by p, we know that $1 = |f|_p = |g|_p \cdot |h|_p$ for all primes p. If $|g|_p \neq 1$, we multiply g with some p^{a_p} and f with p^{-a_p} for some $a_p \in \mathbb{Z}$ such that $|p^a g|_p = 1 = \left|p^{-a} h\right|_p$. Let α be the product of all p^{a_p}, for the finitely many primes p, such that $|g|_p \neq 1$ or $|h|_p \neq 1$. Then $f = (\alpha g) \cdot (\alpha^{-1} h)$ and $|\alpha g|_p = 1 = \left|\alpha^{-1} f\right|_p$ for all primes p. Hence, $\alpha g, \alpha^{-1} h \in \mathbb{Z}[x]$, and since f is irreducible in $\mathbb{Z}$ it follows that g or h must be constant. Therefore, f is irreducible in $\mathbb{Q}[x]$.

Actually the height will just be a normalized form of the Mahler measure, but this normalization (and formulation) will enable us to extend it to much more general settings.
Recall that in view of Theorem 2.2.26, the product formula for the number field K 2.2.16 reads

$$\prod_{v \in M_K} |\alpha|_v^{d_v} = 1 \quad \text{for all } \alpha \in K^*.$$

Theorem 2.3.4. *Let $\alpha \in \overline{\mathbb{Q}}$ be arbitrary with minimal polynomial $f(x) = a_d x^d + \ldots + a_0 = a_d(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_d) \in \mathbb{Z}[x]$. Then we have*

$$M(\alpha) = \prod_{v \in M_{\mathbb{Q}(\alpha)}} \max\{1, |\alpha|_v^{d_v}\}.$$

Proof. If $\alpha = 0$, then both sides are equal to 1. So we assume from now on that $\alpha \in \overline{\mathbb{Q}}^*$. The definition of the Mahler measure and the normalization of the archimedean absolute values, implies

$$M(\alpha) = |a_d| \cdot \prod_{i=1}^{d} \max\{1, |\alpha_i|\} = |a_d| \cdot \prod_{\substack{v \in M_{\mathbb{Q}(\alpha)} \\ v \mid \infty}} \max\{1, |\alpha|_v^{d_v}\}.$$

Hence, we are left to prove

$$|a_d| = \prod_{\substack{v \in M_{\mathbb{Q}(\alpha)} \\ v \nmid \infty}} \max\{1, |\alpha|_v^{d_v}\}. \tag{2.14}$$

To this end, let $K/\mathbb{Q}$ be a Galois extension with $\alpha \in K$ (so you may take the Galois closure of $\mathbb{Q}(\alpha)$). The product formula predicts

$$\begin{aligned} 1 = \prod_{w \in M_K} |a_d|_w^{d_w} &= \prod_{\substack{w \in M_K \\ w \mid \infty}} |a_d|_w^{d_w} \cdot \prod_{\substack{w \in M_K \\ w \nmid \infty}} |a_d|_w^{d_w} \\ &\overset{a_d \in \mathbb{Z}}{=} |a_d|^{\sum_{w \in M_K, w \mid \infty} d_w} \cdot \prod_{\substack{w \in M_K \\ w \nmid \infty}} |a_d|_w^{d_w} \overset{2.2.14}{=} |a_d|^{[K:\mathbb{Q}]} \cdot \prod_{\substack{w \in M_K \\ w \nmid \infty}} |a_d|_w^{d_w}. \end{aligned} \tag{2.15}$$

By assumption all Galois conjugates $\alpha_1, \ldots, \alpha_d$ of α are in K. Since moreover the coefficients of f are coprime, the Gauß-Lemma 2.3.2 tells us

$$1 = |f(x)|_w = |a_d|_w \cdot \prod_{i=1}^{d} |x - \alpha_i|_w = |a_d|_w \cdot \prod_{i=1}^{d} \max\{1, |\alpha_i|_w\} \quad \forall\, w \in M_K,\ w \nmid \infty.$$

This implies

$$1 = \prod_{\substack{w\in M_K\\ w\nmid\infty}} |a_d|_w^{d_w} \cdot \prod_{\substack{w\in M_K\\ w\nmid\infty}} \prod_{i=1}^{d} \max\{1, |\alpha_i|_w^{d_w}\}$$

$$\overset{(2.15)}{\Longrightarrow} \quad |a_d|^{[K:\mathbb{Q}]} = \prod_{\substack{w\in M_K\\ w\nmid\infty}} \prod_{i=1}^{d} \max\{1, |\alpha_i|_w^{d_w}\}. \tag{2.16}$$

For each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, and all $w \in M_K$, $w \mid v$ for some $v \in M_{\mathbb{Q}(\alpha)}$, the function $w \circ \sigma$ is again an absolute value on K extending the same absolute value on $\mathbb{Q}$ as v does. We will apply the following facts. Fact (A): Since $K/\mathbb{Q}$ is Galois, we know from Lemma 2.2.11 and Theorem 2.2.26 that $d_{w\circ\sigma} = d_w$. Fact (B): Since $w \mid v$ we have $|\alpha|_w^{d_w} = |\alpha|_v^{d_{w|v}d_v}$. Fact (C): For every $i \in \{1, \dots, d\}$ there are precisely $[K : \mathbb{Q}(\alpha)] = [K : \mathbb{Q}]/d$ embeddings $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\alpha) = \alpha_i$. Fact (D): σ permutes the elements in M_K^{fin} (this is $\nu \mapsto \nu \circ \sigma$ is bijective on M_K^{fin} for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$[3]). This gives us

$$\prod_{\substack{w\in M_K\\ w\nmid\infty}} \prod_{i=1}^{d} \max\{1, |\alpha_i|_w^{d_w}\} \overset{(C)}{=} \prod_{\substack{w\in M_K\\ w\nmid\infty}} \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} \max\{1, |\sigma(\alpha)|_w^{d_w}\}^{d/[K:\mathbb{Q}]}$$

$$\overset{(A)}{=} \prod_{\substack{w\in M_K\\ w\nmid\infty}} \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} \max\{1, |\alpha|_{w\circ\sigma}^{d_{w\circ\sigma}}\}^{d/[K:\mathbb{Q}]} \overset{(D)}{=} \prod_{\sigma\in\mathrm{Gal}(K/\mathbb{Q})} \prod_{\substack{w\in M_K\\ w\nmid\infty}} \max\{1, |\alpha|_w^{d_w}\}^{d/[K:\mathbb{Q}]}$$

$$= \prod_{\substack{w\in M_K\\ w\nmid\infty}} \max\{1, |\alpha|_w^{d_w}\}^d = \prod_{\substack{v\in M_{\mathbb{Q}(\alpha)}\\ v\nmid\infty}} \prod_{\substack{w\in M_K\\ w|v}} \max\{1, |\alpha|_w^{d_w}\}^d$$

$$\overset{(B)}{=} \prod_{\substack{v\in M_{\mathbb{Q}(\alpha)}\\ v\nmid\infty}} \prod_{\substack{w\in M_K\\ w|v}} \max\{1, |\alpha|_v^{d_w}\}^d \overset{(B)}{=} \prod_{\substack{v\in M_{\mathbb{Q}(\alpha)}\\ v\nmid\infty}} \max\{1, |\alpha|_v^{d_v}\}^{d\sum_{w\in M_K, w|v} d_{w|v}}$$

$$\overset{2.2.14}{=} \prod_{\substack{v\in M_{\mathbb{Q}(\alpha)}\\ v\nmid\infty}} \max\{1, |\alpha|_v^{d_v}\}^{d\cdot[K:\mathbb{Q}(\alpha)]} = \prod_{\substack{v\in M_{\mathbb{Q}(\alpha)}\\ v\nmid\infty}} \max\{1, |\alpha|_v^{d_v}\}^{[K:\mathbb{Q}]}.$$

Combining this with (2.16) proves (2.14) and hence the theorem. □

With Theorem 2.3.4 we see that the archimedean absolute value does not play any exceptional role in the definition of the Mahler measure. Hence, if the archimedean distance between two algebraic numbers is bounded in terms of the Mahler measure, then the p-adic distance should be bounded in terms of the Mahler measure as well.
The same calculation as in the proof of Theorem 2.3.4 also proves:

Lemma 2.3.5. *Let $\alpha \in \overline{\mathbb{Q}}$ be arbitrary, and let K be any number field containing α. Then*

$$\left(\prod_{v\in M_{\mathbb{Q}(\alpha)}} \max\{1, |\alpha|_v\}^{d_v}\right)^{1/[\mathbb{Q}(\alpha):\mathbb{Q}]} = \left(\prod_{w\in M_K} \max\{1, |\alpha|_v\}^{d_v}\right)^{1/[K:\mathbb{Q}]}.$$

[3] There is a pretty obvious inverse map...

Definition 2.3.6. For all $\alpha \in \overline{\mathbb{Q}}$ the *absolute multiplicative Weil-height* of α is defined as $H(\alpha) = \left(\prod_{v \in M_K} \max\{1, |\alpha|_v\}^{d_v}\right)^{1/[K:\mathbb{Q}]}$, for any number field K containing α. In the same notation, the *absolute logarithmic Weil-height* of α is $h(\alpha) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log(\max\{1, |\alpha|_v\})$.

Remark 2.3.7.

- We have seen in Lemma 2.3.5 that the height is indeed well-defined.
- Obviously we have $H(\alpha) = \exp(h(\alpha))$ for all $\alpha \in \overline{\mathbb{Q}}$.
- We have $H(\alpha) = M(\alpha)^{1/[\mathbb{Q}(\alpha):\mathbb{Q}]}$ and $h(\alpha) = \frac{1}{[\mathbb{Q}(\alpha):\mathbb{Q}]} \log(M(\alpha))$. So why does this deserves a new definition? This is justified, since the definition of the height is much more flexible than the definition of the Mahler measure: Not every algebraic object defined over a number field has a minimal polynomial, but everything has a bunch of absolute values! So without any difficulties we can (and will) extend the height to polynomials, and to points in higher dimensions.

  Moreover, with Theorem 2.3.4 we see that the archimedean absolute value does not play any exceptional role in the definition of the Mahler measure (and obviously not in the definition of the height). Hence, if the archimedean distance between two algebraic numbers is bonded in terms of the Mahler measure, then the p-adic distance should be bounded in terms of the Mahler measure as well.

The reformulation of Northcott's theorem, now reads.

Theorem 2.3.8 (Northcott)**.** *For any $A, B \in \mathbb{R}$ there are at most finitely many algebraic numbers α, with $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq A$ and $h(\alpha) < B$, resp. $H(\alpha) < B$.*

Lemma 2.3.9. *Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^*$ be arbitrary, and with h we denote the absolute logarithmic Weil-height (from now on only called* height*). Then*

(a) $h(\alpha_1) \geq 0$, and $h(\alpha_1) = 0$ if and only if α_1 is a root of unity.

(b) $h(\alpha_1 \cdot \zeta) = h(\alpha_1)$ for all roots of unity ζ.

(c) $h(\alpha_1^r) = |r| \cdot h(\alpha_1)$ for all $r \in \mathbb{Q}$.

(d) $h(\alpha_1 + \ldots + \alpha_n) \leq h(\alpha_1) + \ldots + h(\alpha_n) + \log(n)$.

(e) $h(\alpha_1 \cdot \ldots \cdot \alpha_n) \leq h(\alpha_1) + \ldots + h(\alpha_n)$.

Proof. Part (a) is just a reformulation of Kronecker's Theorem 2.1.12, since the height vanishes precisely when the Mahler measure is 1. We will now prove part (d). The other statements are given as exercises.
Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^*$ be arbitrary, and let K be any number field containing all the α_i's. We denote the degree of K by d. The height of $\alpha_1 + \ldots + \alpha_n$ collects information of all possible absolute values of this number. So we should start with estimates for the absolute values of $\alpha_1 + \ldots + \alpha_n$. For $v \in M_K$ the (ultrametric) triangular inequality implies

$$|\alpha_1 + \ldots + \alpha_n|_v \leq \begin{cases} \max_{1 \leq i \leq n} |\alpha_i|_v & \text{if } v \nmid \infty \\ n \cdot \max_{1 \leq i \leq n} |\alpha_i|_v & \text{if } v \mid \infty. \end{cases} \tag{2.17}$$

(The first estimate follows from the definition of the ultrametric triangular inequality, which holds (again by definition) for all non-archimedean absolute values. For the second estimate,

just note that the archimedean absolute values behave precisely as the standard absolute value on $\mathbb{C}$.) Now the result follows from a dry calculation, which starts in a moment. Recall that we have $\frac{1}{d}\sum_{v|\infty} d_v = 1$ (cf. 2.2.14 and 2.2.26). Let's finally prove the claimed inequality:

$$\begin{aligned}
h(\alpha_1+\ldots+\alpha_n) &= \frac{1}{d}\sum_{v\in M_K} d_v \log(\max\{1,|\alpha_1+\ldots+\alpha_n|_v\}) \\
&= \frac{1}{d}\sum_{\substack{v\in M_K\\ v|\infty}} d_v \log(\max\{1,|\alpha_1+\ldots+\alpha_n|_v\}) + \frac{1}{d}\sum_{\substack{v\in M_K\\ v\nmid\infty}} d_v \log(\max\{1,|\alpha_1+\ldots+\alpha_n|_v\}) \\
&\overset{(2.17)}{\leq} \frac{1}{d}\sum_{\substack{v\in M_K\\ v|\infty}} d_v \log(\max\{1,n\max_{1\leq i\leq n}|\alpha_i|_v\}) + \frac{1}{d}\sum_{\substack{v\in M_K\\ v\nmid\infty}} d_v \log(\max\{1,\max_{1\leq i\leq n}|\alpha_i|_v\}) \\
&\leq \frac{1}{d}\sum_{\substack{v\in M_K\\ v|\infty}} d_v \log(n\cdot\max\{1,\max_{1\leq i\leq n}|\alpha_i|_v\}) + \frac{1}{d}\sum_{\substack{v\in M_K\\ v\nmid\infty}} d_v \log(\max\{1,\max_{1\leq i\leq n}|\alpha_i|_v\}) \\
&= \underbrace{\frac{1}{d}\sum_{\substack{v\in M_K\\ v|\infty}} d_v \log(n)}_{=\log(n)} + \frac{1}{d}\sum_{v\in M_K} d_v \log(\max\{1,\max_{1\leq i\leq n}|\alpha_i|_v\}) \\
&\leq \log(n) + \sum_{i=1}^{n}\frac{1}{d}\sum_{v\in M_K} d_v\log(\max\{1,|\alpha_i|_v\}) = \log(n)+\sum_{i=1}^{n} h(\alpha_i).
\end{aligned}$$

This concludes the proof of part (d). □

Following Remark 2.3.7 we can now (most elegantly) extend Liouville's theorem to non-archimedean absolute values.

Theorem 2.3.10. *Let $\alpha,\beta\in\overline{\mathbb{Q}}$ be arbitrary with $\alpha\neq\beta$. Denote the degree of α by d and the degree of β by k. Let $S\subseteq M_{\mathbb{Q}(\alpha,\beta)}$ be a finite set. Then we have*

$$\prod_{v\in S}\min\{1,|\alpha-\beta|_v^{d_v}\} \geq \frac{1}{2^{kd}M(\alpha)^k M(\beta)^d}.$$

Proof. It is $\alpha-\beta\neq 0$ and hence, by Lemma 2.3.9 $H(\alpha-\beta)=H((\alpha-\beta)^{-1})$. Now we calculate

$$\begin{aligned}
H((\alpha-\beta)^{-1}) &= \prod_{v\in M_{\mathbb{Q}(\alpha,\beta)}}\max\{1,\left|\frac{1}{\alpha-\beta}\right|_v^{d_v/[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]}\} = \prod_{v\in M_{\mathbb{Q}(\alpha,\beta)}}\frac{1}{\min\{1,|\alpha-\beta|_v\}^{d_v/[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]}} \\
&\geq \prod_{v\in S}\frac{1}{\min\{1,|\alpha-\beta|_v\}^{d_v/[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]}}.
\end{aligned}$$

This implies

$$\begin{aligned}
\prod_{v\in S}\min\{1,|\alpha-\beta|_v\}^{d_v} &\geq \frac{1}{H(\alpha-\beta)^{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]}} \overset{2.3.9}{\geq} \frac{1}{(2H(\alpha)H(\beta))^{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]}} \\
&\overset{2.3.7}{=} \frac{1}{2^{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]}M(\alpha)^{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]/[\mathbb{Q}(\alpha):\mathbb{Q}]}M(\beta)^{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]/[\mathbb{Q}(\beta):\mathbb{Q}]}}.
\end{aligned}$$

The standard inequalities $\frac{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]}{[\mathbb{Q}(\alpha):\mathbb{Q}]}\leq k$, $\frac{[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]}{[\mathbb{Q}(\beta):\mathbb{Q}]}\leq d$, and $[\mathbb{Q}(\alpha,\beta):\mathbb{Q}]\leq kd$ prove the theorem. □

The following immediate consequence is the direct (and effective) generalization of Liouville's Theorem for number fields.

Corollary 2.3.11. *Let $\alpha \in \overline{\mathbb{Q}}$ be of degree d, and fix a number field K of degree k. Moreover, let $S \subseteq M_{K(\alpha)}$ be a finite set. Then for all $\beta \in K \setminus \{\alpha\}$ we have*

$$\prod_{v \in S} \min\{1, |\alpha - \beta|_v^{d_v}\} \geq \frac{c_K(\alpha)}{M(\beta)^{[K(\alpha):\mathbb{Q}(\beta)]}} \geq \frac{c_K(\alpha)}{M(\beta)^{d[K:\mathbb{Q}(\beta)]}} = \frac{c_K(\alpha)}{H(\beta)^{dk}},$$

where $c_K(\alpha) = \frac{1}{2^{kd} M(\alpha)^k}$.

Note that the dependence on K is actually just a dependence on the degree of K. Moreover, this gives us a quite good feeling on how the statement of Roth's theorem for arbitrary number fields, and arbitrary absolute values should look like. Namely, for a fixed number field K we should have something like

$$\forall\ \alpha \in \overline{\mathbb{Q}},\ \forall\ \varepsilon > 0,\ \forall\ S \subseteq M_{K(\alpha)} \text{ finite}, \exists\ c_K(\alpha, \varepsilon, S) > 0 \text{ such that}$$
$$\prod_{v \in S} \min\{1, |\alpha - \beta|_v^{d_v}\} > \frac{c_K(\alpha, \varepsilon, S)}{H(\beta)^{[K:\mathbb{Q}](2+\varepsilon)}} \quad \forall\ \beta \in K \setminus \{\alpha\}. \quad \text{(RT6)}$$

As seen in the exercises, this is equivalent to the statement

$$\forall\ \alpha \in \overline{\mathbb{Q}},\ \forall\ \varepsilon > 0,\ \forall\ S \subseteq M_{K(\alpha)} \text{ finite, the set}$$
$$\left\{ \beta \in K |\ \prod_{v \in S} \min\{1, |\alpha - \beta|_v\}^{d_v} < H(\beta)^{-[K:\mathbb{Q}](2+\varepsilon)} \right\} \text{ is finite.} \quad \text{(RT7)}$$

Notice that in sharp contrast to the constant in the general Liouville's theorem 2.3.11, the constant $c_K(\alpha, \varepsilon, S)$ from (RT6) is completely ineffective. That is, for no choice of K, α, ε, and S, any constant is known that satisfies (RT6).

Definition 2.3.12. Let $\overline{\mathbb{Q}}[x_1, \ldots, x_n]$ be the polynomial ring over $\overline{\mathbb{Q}}$ in n variables. The multiplicative (resp. logarithmic) absolute Weil-height of $f \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ is given by

$$H(f) = \prod_{v \in M_K} \max\{1, |f|_v\}^{d_v/[K:\mathbb{Q}]} \quad \text{(resp. } h(f) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v \log\left(\max\{1, |f|_v\}\right) \text{)},$$

where K is any number field, with $f \in K[x_1, \ldots, x_n]$.

As before we can conclude that the height of a polynomial is well-defined. We know that $\overline{\mathbb{Q}} \subseteq \overline{\mathbb{Q}}[x_1, \ldots, x_n]$, and it is obvious that the height for polynomials and the height for algebraic numbers coincide for constant polynomials.

Definition 2.3.13. Let K be a field and let $n \in \mathbb{N}$ be arbitrary. We have an equivalence relation $\sim$ on $K^{n+1} \setminus \{0\}$, given by $(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n)$ if and only if there exists a $\lambda \in K^*$ such that $a_i = \lambda b_i$ for all $i \in \{0, \ldots, n\}$. We set $\mathbb{P}^n(K) = {}^{K^{n+1}\setminus\{0\}}/_{\sim}$ and call this the *projective space* over K of dimension n. The equivalence class of $(a_0, \ldots, a_n)$ in $\mathbb{P}^n(K)$ is denoted by $[a_0 : \ldots : a_n]$.

Proposition 2.3.14. *Let $n \in \mathbb{N}$ be arbitrary. The following function is well-defined:*

$$H : \mathbb{P}^n(\overline{\mathbb{Q}}) \longrightarrow \mathbb{R} \quad ; \quad [a_0 : \ldots : a_n] \mapsto \prod_{v \in M_K} \max_{0 \leq i \leq n} |a_i|_v^{d_v/[K:\mathbb{Q}]},$$

where K is any number field, with $a_0, \ldots, a_n \in K$.

Proof. The value of $H([a_0 : \ldots : a_n])$ could depend on the choice of representative for the equivalence class, and on the choice of number field K. We have to exclude both.
Notice that for $a_0, \ldots, a_n \in \overline{\mathbb{Q}}$, with $a_i = 1$ for some i, the value $\prod_{v \in M_K} \max_{0 \leq i \leq n} |a_i|_v^{d_v/[K:\mathbb{Q}]}$ is equal to $H(a_n x_n + \ldots + a_0)$ for all number fields K, such that $a_0, \ldots, a_n \in K$. Hence, $H([a_0 : \ldots : a_n])$ is indeed independent on the choice of K.
Next, let $\lambda \in \overline{\mathbb{Q}}^*$ be arbitrary, and let K be a number field containing $\lambda, a_0, \ldots, a_n$. Then

$$\begin{aligned}
\prod_{v \in M_K} \max_{0 \leq i \leq n} |\lambda a_i|_v^{d_v/[K:\mathbb{Q}]} &= \prod_{v \in M_K} |\lambda|_v^{d_v/[K:\mathbb{Q}]} \max_{0 \leq i \leq n} |a_i|_v^{d_v/[K:\mathbb{Q}]} \\
&= \left(\prod_{v \in M_K} |\lambda|_v^{d_v} \right)^{1/[K:\mathbb{Q}]} \prod_{v \in M_K} \max_{0 \leq i \leq n} |a_i|_v^{d_v/[K:\mathbb{Q}]} \\
&\overset{2.2.16}{=} \prod_{v \in M_K} \max_{0 \leq i \leq n} |a_i|_v^{d_v/[K:\mathbb{Q}]}.
\end{aligned}$$

It follows that H is well-defined. □

Definition 2.3.15. For all $P \in \mathbb{P}^n$ the *absolute multiplicative Weil-height of P* is given by $H(P)$, for the function H from Proposition 2.3.14. The *absolute logarithmic Weil-height of P* is given by $h(P) = \log(H(P))$.

This is of course a direct extension of the definition of the height on $\overline{\mathbb{Q}}$, since for any $\alpha \in \overline{\mathbb{Q}}$, we have $H(\alpha) = H([\alpha : 1])$. Therefore, we can safely use the same notation for both functions. Again for $\alpha \in \overline{\mathbb{Q}}$ it follows immediately from Theorem 2.3.4, that $H(\sigma(\alpha)) = H(\alpha)$ for all $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\alpha), \mathbb{C})$ (or equivalently for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$). This is also true for points in $\mathbb{P}^n(\overline{\mathbb{Q}})$ for $n \geq 2$.

Lemma 2.3.16. *Let $P = [a_0 : \ldots : a_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Then $\sigma(P) = [\sigma(a_0) : \ldots : \sigma(a_n)]$ is well-defined, and we have $H(P) = H(\sigma(P))$.*

Proof. For any $\lambda \in \overline{\mathbb{Q}}^*$ we have

$$[\sigma(\lambda a_0) : \ldots : \sigma(\lambda a_n)] = [\underbrace{\sigma(\lambda)}_{\in \overline{\mathbb{Q}}^*} \sigma(a_0) : \ldots : \underbrace{\sigma(\lambda)}_{\in \overline{\mathbb{Q}}^*} \sigma(a_n)] = \sigma(P).$$

Hence $\sigma(P)$ is indeed well-defined.
Let $K/\mathbb{Q}$ be any Galois extension containing all Galois conjugates of all the a_i's for $i \in \{0, \ldots, n\}$. For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have that the restriction of σ to K is in $\mathrm{Gal}(K/\mathbb{Q})$. Hence, we may assume $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.
As seen before, for any $v \in M_K$ also $v \circ \sigma \in M_K$. Moreover, since $K/\mathbb{Q}$ is Galois, we have $d_v = d_{v \circ \sigma}$ for all $v \in M_K$, and the map $v \mapsto v \circ \sigma$ is a bijection on M_K ($v \mapsto v \circ \sigma^{-1}$ is an

inverse map). Hence,

$$H(\sigma(P)) = \prod_{v\in M_K} \max_{0\le i\le n} |\sigma(a_i)|_v^{d_v/[K:\mathbb{Q}]} = \prod_{v\in M_K} \max_{0\le i\le n} |a_i|_{v\circ\sigma}^{d_v/[K:\mathbb{Q}]}$$
$$= \prod_{v\in M_K} \max_{0\le i\le n} |a_i|_{v\circ\sigma}^{d_{v\circ\sigma}/[K:\mathbb{Q}]} = \prod_{v\in M_K} \max_{0\le i\le n} |a_i|_v^{d_v/[K:\mathbb{Q}]} = H(P).$$

□

Exercises

Exercise 2.9. Let $\alpha \in \overline{\mathbb{Q}}$ be arbitrary. Prove that $M(\alpha)$ is an algebraic integer.

Exercise 2.10. Prove that the height (multiplicative or logarithmic) of a polynomial in $\overline{\mathbb{Q}}[x_1, \ldots, x_n]$ is well-defined.

Exercise 2.11. Prove statements (b),(c), and (e) in Lemma 2.3.9. Moreover, prove that the inequality in (d) is strict. This is, prove that for every $n \in \mathbb{N}$ there are algebraic numbers $\alpha_1, \ldots, \alpha_n$, such that $h(\alpha_1 + \ldots + \alpha_n) = \log(n) + h(\alpha_1) + \ldots + h(\alpha_n)$.

Exercise 2.12. Let m, n be distinct integers, and let $\alpha \in \overline{\mathbb{Q}}^*$ be such that α^n is a Galois conjugate of α^m. Prove that α is a root of unity.

Exercise 2.13. Here you can prove (using an enormous shortcut) a result which is originally due to Enrico Bombieri and Umberto Zannier: Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic integer, such that all Galois conjugates of α lie in $\mathbb{Q}_p$ for some fixed prime number p (such an element is called totally p-adic integer). Assume furthermore that $\alpha \neq \alpha^p$.

(a) Use Exercise 2.8 to prove that $h((\alpha - \alpha^p)^{-1}) \ge \log(p)$.

(b) Conclude $h(\alpha) \ge \frac{\log(p/2)}{p-1}$.

(c) Conclude that the only possible roots of unity in $\mathbb{Q}_p$ are the $p-1$-st roots of unity.

(d) Conclude that Lehmer's conjecture is true for all totally p-adic numbers, for any $p \ge 3$.

(e) Prove that Lehmer's conjecture is also true for all totally 2-adic numbers.

2.4 Siegel's Lemma

Large parts of this section are shamelessly stolen from [5]. For the whole section we will fix the following notation.

Notation 2.4.1. Let $N > M > 0$ be integers, and let

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1N} \\ \vdots & \ldots & \vdots \\ a_{M1} & \ldots & a_{MN} \end{pmatrix} \in M_{M\times N}(\overline{\mathbb{Q}})$$

be a matrix with entries in $\overline{\mathbb{Q}}$. We are looking for a "small" solution of the equation

$$A \cdot \mathbf{x} = \mathbf{0}. \tag{2.18}$$

Since $N > M$ there are more variables than equation, and hence there is a non-trivial ($\mathbf{x} \neq \mathbf{0}$) solution of (2.18). Without loss of generality we assume that A does not have a zero row. We define

$$L_j = a_{j1}x_1 + \ldots + a_{jN}x_N \in \overline{\mathbb{Q}}[x_1, \ldots, x_N] \setminus \{0\} \quad \forall\, j \in \{1, \ldots, M\},$$

where $\overline{\mathbb{Q}}[x_1, \ldots, x_N]$ is the polynomial ring over $\overline{\mathbb{Q}}$ with variables $x_1, \ldots, x_N$. Now, obviously, solving (2.18) is equivalent to find some $\mathbf{b} \in \overline{\mathbb{Q}}^N$ such that $L_j(\mathbf{b}) = 0$ for all $j \in \{1, \ldots, M\}$. How do we measure the size of an algebraic object in this section? By heights! And maybe you can guess by now what's the height of A.
Let K be a number field containing all entries a_{ij} of the matrix A. For $v \in M_K$ define $|A|_v = \max_{i,j} |a_{ij}|_v$. Then the height of A is given by

$$H(A) = \prod_{v \in M_K} \max\{1, |A|_v\}^{d_v/[K:\mathbb{Q}]}.$$

Since the coefficients of each L_j come from a subset of the entries of A, we immediately conclude

$$H(A) \geq \max_{1 \leq j \leq M} H(L_j). \tag{2.19}$$

We will give three results in this direction. First, we assume that the matrix A and the solution vector have entries in $\mathbb{Z}$.

Proposition 2.4.2 (Siegel's Lemma for $(\mathbb{Z}, \mathbb{Z})$)**.** *Let $A \in M_{M \times N}(\mathbb{Z})$. Then there is a solution $\mathbf{b} \in \mathbb{Z}^N \setminus \{\mathbf{0}\}$ of* (2.18)*, such that $H(\mathbf{b}) \leq (NH(A))^{\frac{M}{N-M}}$.*

Proof. Before we start the proof, please note that this formulation is slightly too advanced, since $H(A)$ is just the maximal modulus of the entries of A, and $H(\mathbf{b})$ is the maximal modulus of the entries of $\mathbf{b}$.
The proof is an application of the box principle. However, before we come to the nice conclusion, we will do the necessary computations. To ease notation we set

$$X = \left\lfloor (NH(A))^{\frac{M}{N-M}} \right\rfloor \in \mathbb{N}.$$

For any $a \in \mathbb{R}$ we define $a^+ = \max\{a, 0\}$ and $a^- = \max\{-a, 0\}$. Then we get for all $a \in \mathbb{R}$ the equations $a = a^+ - a^-$ and $|a| = a^+ + a^-$. Similarly, for each of our linear forms $L_1, \ldots, L_M$ we define $L_j^+ = \sum_{i=1}^N a_{ji}^+$, $L_j^- = \sum_{i=1}^N a_{ji}^-$ and $\widetilde{L_j} = L_j^+ + L_j^-$. It is immediately clear that

$$\widetilde{L_j} = \sum_{i=1}^{N} |a_{ji}| \leq N \cdot H(L_j) \leq N \cdot H(A) \qquad \forall\, j \in \{1, \ldots, M\}. \tag{2.20}$$

Note also, that by definition of X, we have $X + 1 > (NH(A))^{\frac{M}{N-M}}$. We apply this to achieve

$$\begin{aligned}(X+1)^N &= (X+1)^M \cdot (X+1)^{N-M} > (X+1)^M \cdot \left((NH(A))^{\frac{M}{N-M}}\right)^{N-M} \\ &= ((X+1) \cdot (N \cdot H(A)))^M \overset{(2.20)}{\geq} \prod_{j=1}^{M} \left(\widetilde{L_j} \cdot (X+1)\right) \geq \prod_{j=1}^{M} \left(\widetilde{L_j} \cdot X + 1\right). \end{aligned} \tag{2.21}$$

Actually, the value in the theorem is exactly chosen such that this inequality is true.
Now we will set the stage to apply the box principle. Therefore we estimate the cardinality of

$$A \cdot \{0, \dots, X\}^N := \{A \cdot \mathbf{b} | \mathbf{b} \in \{0, \dots, X\}^N\}.$$

Any element $\mathbf{b} \in \{0, \dots, X\}^N$ satisfies

$$-L_j^- \cdot X \leq L_j(\mathbf{b}) \leq L_j^+ \cdot X.$$

Hence, we can conclude

$$A \cdot \{0, \dots, X\}^N \subseteq [-L_1^- \cdot X, L_1^+ \cdot X] \times \ldots \times [-L_M^- \cdot X, L_M^+ \cdot X].$$

Since the interval $[-L_j^- \cdot X, L_j^+ \cdot X]$ contains precisely $L_j^- \cdot X + L_j^+ \cdot X + 1 = \widetilde{L_j} \cdot X + 1$ integers, we get

$$\left|A \cdot \{0, \dots, X\}^N\right| \leq \prod_{j=1}^{M} (\widetilde{L_j} \cdot X + 1), \tag{2.22}$$

and from (2.21) it follows that

$$\left|A \cdot \{0, \dots, X\}^N\right| \leq \prod_{j=1}^{M} (\widetilde{L_j} \cdot X + 1) < (X+1)^N = \left|\{0, \dots, X\}^N\right|.$$

Hence, the box principle guarantees that there are two distinct elements $\mathbf{t}, \mathbf{s} \in \{0, \dots, X\}^N$ such that $A \cdot \mathbf{t} = A \cdot \mathbf{s}$. Then $\mathbf{b} = \mathbf{t} - \mathbf{s} \in \{-X, \dots, X\}^N \setminus \{\mathbf{0}\}$ satisfies $A \cdot \mathbf{b} = \mathbf{0}$. Since the condition $\mathbf{b} \in \{-X, \dots, X\}^N$ is precisely the same as $\mathbf{b} \in \mathbb{Z}^N$, with $H(\mathbf{b}) \leq X$, the proposition is proved. □

Remark 2.4.3. One can slightly improve on this result, be replacing the factor N by $\sqrt{N}$.

Next we aim for a version of Siegel's lemma, where A has entries in a number field and the small solution has entries in $\mathbb{Z}$.

Lemma 2.4.4. *Let K be a number field. For each $v \in M_K$ we fix an element $\alpha_v \in K$ and a real number $c_v \geq 1$, such that $c_v = 1$ for all but finitely many $v \in M_K$. Then*

$$|\{\alpha \in K | \ |\alpha - \alpha_v|_v \leq c_v \quad \forall\ v \in M_K\}| \leq \left(2C^{1/[K:\mathbb{Q}]} + 1\right)^{[K:\mathbb{Q}]},$$

where $C = \prod_{v \in M_K} c_v^{d_v}$.

Proof. We start by fixing some notation. Let $[K : \mathbb{Q}] = d$ and denote by $\sigma_1, \dots, \sigma_r$ the real embeddings of K and by $\sigma_{r+1}, \overline{\sigma_{r+1}}, \dots, \sigma_{r+s}, \overline{\sigma_{r+s}}$ the complex embeddings of K, such that $d = r + 2s$. A full set of non-equivalent archimedean absolute values on K is then given by $|.|_{\sigma_1} = |\sigma_1(.)|, \dots, |.|_{\sigma_{r+s}} = |\sigma_{r+s}(.)|$. For any $\alpha \in K$ and $\varepsilon > 0$ we define

$$B(\alpha, \varepsilon) = \{\mathbf{x} = (x_1, \dots, x_{r+s}) \in \mathbb{R}^r \times \mathbb{C}^s | \ |x_i - \sigma_i(\alpha)| < \varepsilon c_{\sigma_i} \ \forall\ i \in \{1, \dots, r+s\}\}.$$

Moreover, we define $\mathcal{A} = \{\alpha \in K | \ |\alpha - \alpha_v|_v \leq c_v \quad \forall\ v \in M_K\}$, which is precisely the set whose cardinality we want to estimate. Lastly, we set

$$\epsilon = \frac{1}{2} C^{-1/d}. \tag{2.23}$$

Now let $\alpha, \beta \in \mathcal{A}$ and assume there exists an $\mathbf{x} = (x_1, \dots, x_{r+s}) \in B(\alpha, \epsilon) \cap B(\beta, \epsilon)$. Then for all $i \in \{1, \dots, r+s\}$ we have

$$|\alpha - \beta|_{\sigma_i} = |\sigma_i(\alpha) - \sigma_i(\beta)| \leq |x_i - \sigma_i(\alpha)| + |x_i - \sigma_i(\beta)| < 2\epsilon c_{\sigma_i}$$

for the archimedean absolute values, and for all $v \in M_K^{\text{fin}}$ we have (since $\alpha, \beta \in \mathcal{A}$)

$$|\alpha - \beta|_v = |\alpha - \alpha_v - (\beta - \alpha_v)|_v \leq \max\{|\alpha - \alpha_v|_v, |\beta - \alpha_v|_v\} \leq c_v.$$

We can conclude that

$$\prod_{v \in M_K} |\alpha - \beta|_v^{d_v} < (2\epsilon)^d \prod_{v \in M_K} c_v^{d_v} = (2\epsilon)^d \cdot C \overset{(2.23)}{=} 1.$$

By the product formula 2.2.16, this is only possible if $\alpha = \beta$. In conclusion we have just seen, that for two different points $\alpha, \beta \in \mathcal{A}$, the boxes $B(\alpha, \epsilon)$ and $B(\beta, \epsilon)$ are disjoint. This implies

$$\text{Vol}\left(\cup_{\alpha \in \mathcal{A}} B(\alpha, \epsilon)\right) = |\mathcal{A}| \cdot \text{Vol}\left(B(0, \epsilon)\right) = |\mathcal{A}| \cdot \epsilon^d \,\text{Vol}\left(B(0,1)\right). \tag{2.24}$$

Here we use the usual volume on $\mathbb{R}^r \times \mathbb{C}^s$ and the obvious fact that the volume of some $B(\alpha, \epsilon)$ does not depend on the point α.
If $(x_1, \dots, x_{r+s}) \in \cup_{\alpha \in \mathcal{A}} B(\alpha, \epsilon)$, then for all $i \in \{1, \dots, r+s\}$ we have that for some $\alpha \in \mathcal{A}$

$$|x_i - \sigma_i(\alpha_{\sigma_i})| \leq |x_i - \sigma_i(\alpha)| + \underbrace{|\sigma_i(\alpha) - \sigma_i(\alpha_{\sigma_i})|}_{= |\alpha - \alpha_{\sigma_i}|_{\sigma_i}} \leq (1+\epsilon) c_{\sigma_i}.$$

This just means, that

$$\begin{aligned} \cup_{\alpha \in \mathcal{A}} B(\alpha, \epsilon) \subseteq & \prod_{i=1}^{r} \{x \in \mathbb{R} \mid\ |x - \sigma_i(\alpha_{\sigma_i})| \leq (1+\epsilon) c_{\sigma_i}\} \\ & \times \prod_{i=1}^{s} \{x \in \mathbb{C} \mid\ |x - \sigma_{r+i}(\alpha_{\sigma_{r+i}})| \leq (1+\epsilon) c_{\sigma_{r+i}}\}, \end{aligned}$$

and the volume of the right hand side is equal to $\text{Vol}\left(B(0, 1+\epsilon)\right) = (1+\epsilon)^d \cdot \text{Vol}(B(0,1))$, since we may shift the center of the box to the point $(0, \dots, 0)$ without changing the volume. Hence, we have

$$|\mathcal{A}| \cdot \epsilon^d \,\text{Vol}\left(B(0,1)\right) \overset{(2.24)}{=} \text{Vol}\left(\cup_{\alpha \in \mathcal{A}} B(\alpha, \epsilon)\right) \leq (1+\epsilon)^d \cdot \text{Vol}\left(B(0,1)\right),$$

which implies

$$|\mathcal{A}| \leq \left(\frac{1+\epsilon}{\epsilon}\right)^d \overset{(2.23)}{=} \left(2C^{1/d} + 1\right)^d,$$

concluding the proof. □

Remark 2.4.5. Now we can generalize the first version of Siegel's Lemma. In the situation considered next, we are given a matrix A with entries in a number field K and we want to solve the usual equation (2.18) with a vector in $\mathbb{Z}^N$. But the usual assumption $M < N$ is clearly too weak to guarantee the existence of such a solution. Assume $M = 1$ and $N = 3$. Then the matrix is just a single row, and we want to solve a single linear equation with three variables. Taking $1 \cdot x_1 + \sqrt[3]{2} \cdot x_2 + (\sqrt[3]{2})^2 \cdot x_3 = 0$ shows that there are in general no solutions, because the degree of $\sqrt[3]{2}$ is too large. (If there was an integral solution to this equation, it would yield a quadratic polynomial with root $\sqrt[3]{2}$.) Hence, we need at least the assumption $[K : \mathbb{Q}] \cdot M < N$ to guarantee an integral solution. This is indeed sufficient.

Proposition 2.4.6 (Siegel's Lemma for $(K,\mathbb{Z})$)**.** *Let K be a number field of degree d, and assume $A \in M_{M\times N}(K)$. Moreover, we assume that the positive integers M, N satisfy $d\cdot M < N$. Then there is a solution $\mathbf{b} \in \mathbb{Z}^N \setminus \{\mathbf{0}\}$ of (2.18), such that $H(\mathbf{b}) \leq (NH(A))^{\frac{dM}{N-dM}}$.*

Proof. We want to mimic the proof from Proposition 2.4.2 and want to apply the box principle in the very same fashion. Again we ease notation and set $X = \left\lfloor (NH(A))^{\frac{dM}{N-dM}} \right\rfloor$. Then as before we want to estimate the cardinality of

$$A\cdot\{0,\dots,X\}^N := \{A\cdot\mathbf{b} | \mathbf{b}\in\{0,\dots,X\}^N\}.$$

We can estimate the cardinality of the set above, if for all $j\in\{1,\dots,M\}$ we can estimate

$$L_j(\{0,\dots,X\}^N) := \{L_j(\mathbf{b}) | \mathbf{b}\in\{0,\dots,X\}^N\}.$$

This will be done by the preceding lemma. We fix for the moment an $j\in\{1,\dots,M\}$ and define for all $v\in M_K$

$$\alpha_v = \begin{cases} L_j(\frac{X}{2},\dots,\frac{X}{2}) & \text{if } v\mid\infty \\ 0 & \text{if } v\nmid\infty \end{cases}$$
$$c_v = \begin{cases} \frac{1}{2}NX\max\{1,|L_j|_v\} & \text{if } v\mid\infty \\ \max\{1,|L_j|_v\} & \text{if } v\nmid\infty. \end{cases}$$

Then $c_v\geq 1$ for all $v\in M_K$, and $c_v = 1$ for all but finitely many v. Furthermore, we calculate

$$\begin{aligned} C = \prod_{v\in M_K} c_v^{d_v} &= (\frac{1}{2}NX)^d\cdot\prod_{v\in M_K}\max\{1,|L_j|_v^{d_v}\} = (\frac{1}{2}NX)^d\cdot H(L_j)^d \\ &\overset{(2.19)}{\leq} (\frac{1}{2}NXH(A))^d. \end{aligned} \tag{2.25}$$

Hence, we know from Lemma 2.4.4 that

$$\left|\underbrace{\{\alpha\in K|\ |\alpha-\alpha_v|_v\leq c_v \quad \forall\, v\in M_K\}}_{=\mathcal{A}}\right| \leq \left(2C^{1/d}+1\right)^d \overset{(2.25)}{\leq} (NXH(A)+1)^d. \tag{2.26}$$

We claim that $L_j(\{0,\dots,X\}^N)\subseteq\mathcal{A}$ (actually we have chosen the α_v and c_v precisely such that this is the case). Indeed, let $\mathbf{b}=(b_1,\dots,b_N)\in\{0,\dots,X\}^N$ be arbitrary. Then, applying that $b_i-\frac{X}{2}\in[-\frac{X}{2},\frac{X}{2}]$, and that the non-archimedean absolute value of an integer is at most 1, we get

$$|L_j(\mathbf{b})-\alpha_v|_v = \begin{cases} \left|L_j(b_1-\frac{X}{2},\dots,b_N-\frac{X}{2})\right|_v \leq |L_j|_v\, N\max_{1\leq i\leq N}\left|b_i-\frac{X}{2}\right|_v \leq c_v & \text{if } v\mid\infty \\ |L_j(b_1,\dots,b_N)|_v \leq \max_{1\leq i\leq N}|a_{ji}b_i|_v \leq |L_j|_v \leq c_v & \text{if } v\nmid\infty. \end{cases}$$

This proves the claim, and we conclude that for all $j\in\{1,\dots,M\}$ we have

$$\left|L_j(\{0,\dots,X\}^N)\right| \leq |\mathcal{A}| \overset{(2.26)}{\leq} (NXH(A)+1)^d.$$

This immediately implies

$$\left|A \cdot \{0, \ldots, X\}^N\right| \leq (NXH(A)+1)^{dM}, \tag{2.27}$$

and we can finally proceed exactly as in the proof of Proposition 2.4.2. Since by the definition of X and (2.27) we have

$$\begin{aligned}\left|A \cdot \{0, \ldots, X\}^N\right| &\leq (NXH(A)+1)^{dM} \leq (NH(A))^{dM}(X+1)^{dM} \\ &\overset{dM<N}{<} (X+1)^{N-dM}(X+1)^{dM} = \left|\{0, \ldots, X\}^N\right|.\end{aligned}$$

Hence, the box principle guarantees two different elements $\mathbf{t}, \mathbf{s} \in \{0, \ldots, X\}^N$ such that $A \cdot \mathbf{t} = A \cdot \mathbf{s}$. Setting $\mathbf{b} = \mathbf{s} - \mathbf{t}$ gives a non-trivial solution to (2.18), with $H(\mathbf{b}) \leq X$. □

As a corollary of this last version of Siegel's Lemma we achieve:

Corollary 2.4.7 (Siegel's Lemma for $(K, \mathcal{O}_K)$)**.** *Let K be a number field of degree d and let $A \in M_{M\times N}(K)$. Then there is a solution $\mathbf{b} \in \mathcal{O}_K^N \setminus \{\mathbf{0}\}$ of (2.18), such that $H(\mathbf{b}) \leq c_K(c_K N H(A))^{\frac{M}{N-M}}$, for some constant c_K only depending on K.*

Proof. This is given as an Exercise. Be aware of the fact, that the constant c_K in the theorem, will indeed depend on the field K and not only on d. □

We will give a sample application of Siegel's Lemma.

Corollary 2.4.8. *Let $\alpha \in \overline{\mathbb{Q}}$ be arbitrary. There exists a polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$ and $H(f) \leq M(\alpha)$ (this means that all coefficients of f have absolute value $\leq M(\alpha)$).*

Proof. Let $\alpha \in \overline{\mathbb{Q}}$ be of degree d, and consider the linear equation

$$L(\mathbf{x}) = x_1 + \alpha \cdot x_2 + \ldots + \alpha^{N-1} \cdot x_N = 0.$$

This is we set $M = 1$ in the above notation, and the matrix A consists of the single row $(1, \alpha, \ldots, \alpha^{N-1})$. The height of A (resp. L) is given by

$$\begin{aligned}H(A) &= \prod_{v \in M_{\mathbb{Q}(\alpha)}} \max\{1, \max_{1\leq j\leq N-1}\{\left|\alpha^j\right|_v\}\}^{d_v/d} = \prod_{v\in M_{\mathbb{Q}(\alpha)}} \max\{1, \left|\alpha^{N-1}\right|_v\}^{d_v/d} \\ &= H(\alpha^{N-1}) \overset{2.3.9}{=} H(\alpha)^{N-1}.\end{aligned}$$

Hence, by Siegel's Lemma 2.4.6, there are $b_1, \ldots, b_N \in \mathbb{Z}$, such that $b_1 + \alpha \cdot b_2 + \ldots + \alpha^{N-1} \cdot b_N = 0$, and

$$\max_{1\leq j\leq N} |b_j| \leq (N \cdot H(\alpha)^{N-1})^{\frac{d}{N-d}} = N^{\frac{d}{N-d}} \cdot M(\alpha)^{\frac{N-1}{N-d}} \overset{N\to\infty}{\longrightarrow} M(\alpha).$$

Therefore, for N sufficiently large, we may assume that $\max_{1\leq j\leq N} |b_j| \leq M(\alpha)$. Moreover, by the choice of A, we know that α is a root of the polynomial $f(x) = b_1 + b_2 \cdot x + \ldots + b_N \cdot x^{N-1}$. □

Remark 2.4.9. The bound for the coefficients in Corollary 2.4.8 is sharp: the Mahler measure of a positive integer $a \in \mathbb{N}$ is just a, and any polynomial $f \in \mathbb{Z}[x]$ such that $f(a) = 0$ satisfies $x - a \mid f(x)$. Hence, the coefficient of f with smallest index, is a non-zero multiple of a.

Moreover, note that the polynomial from Corollary 2.4.8 need not to be the minimal polynomial of α (compare the bound from Lemma 2.1.7). As an example we take the polynomial $f(x) = (x+1)^8 + 1$. This is irreducible and has (by the binomial theorem) largest coefficient $\binom{8}{4} = 70$. Since it is irreducible, the Mahler measure of all of its roots is the same. Note that $\zeta_{16} - 1$ is a root of f, where ζ_{16} is a primitive 16-th root of unity. The Mahler measure of $\zeta_{16} - 1$ is however $13,13707...$, which is much smaller than 70.

Definition 2.4.10. Let $P \in \mathbb{C}[x]$ be a polynomial. We write $P(x) = \prod_{z\in\mathbb{C}}(x-z)^{\mathrm{ord}_P(z)}$, with non-negative integers $\mathrm{ord}_P(z)$, which are equal to zero for all but finitely many $z \in \mathbb{C}$. The integer $\mathrm{ord}_P(z)$ is called the *order of P at z*.

In simpler words, the order of $z \in \mathbb{C}$ at $P \in \mathbb{C}[x]$ measures the multiplicity of the root z of P. By the fundamental theorem of Algebra, for every $P \in \mathbb{C}[x]$ there are unique (up to permutation) pairwise distinct $z_1, \dots, z_d \in \mathbb{C}$, and $e_1, \dots, e_d \in \mathbb{N}$ such that

$$P(x) = (x - z_1)^{e_1} \cdot \ldots \cdot (x - z_d)^{e_d}.$$

Then, $\mathrm{ord}_P(z_i) = e_i$ for all $i \in \{1, \dots, d\}$ and $\mathrm{ord}_P(z) = 0$ for all $z \in \mathbb{C} \setminus \{z_1, \dots, z_d\}$. We denote the nth derivative of a polynomial $P \in \mathbb{C}[x]$ by $P^{(n)}$. So in particular $P^{(0)} = P$. Then we have

$$\mathrm{ord}_P(z) = T \quad \Longleftrightarrow \quad P^{(n)}(z) = 0 \quad \forall\, n \in \{0, \dots, T-1\} \text{ and } P^{(T)}(z) \neq 0.$$

Or, rephrasing this, the order of P at α is given by the minimal T such that the Tth derivative of P does not vanish at α.

Proposition 2.4.11. *Let $\alpha \in \overline{\mathbb{Q}}$ be arbitrary of degree d, and let T and L be positive integers, with $L \geq dT$. Then there exists a polynomial $P \in \mathbb{Z}[x] \setminus \{0\}$, such that*

(i) $\deg(P) \leq L$,

(ii) $\mathrm{ord}_P(\alpha) \geq T$, *and*

(iii) $H(P) \leq \left((L+1)L^{T-1}H(\alpha)^L\right)^{dT/L+1-dT}$.

Proof. We imitate the proof of Corollary 2.4.8. That the order of P at α is at least T means that $P(\alpha) = P^{(1)}(\alpha) = \ldots = P^{(T-1)}(\alpha) = 0$. Hence, the coefficients of P satisfy T linear equations defined over $\mathbb{Q}(\alpha)$. More precisely, the nth derivative of a polynomial $P(x) = b_L x^L + \ldots + b_0$ (which is obviously of degree at most L) is given by

$$P^{(n)}(x) = b_L \cdot (\prod_{i=0}^{n-1}(L-i))x^{L-n} + b_{L-1} \cdot (\prod_{i=0}^{n-1}(L-1-i))x^{L-1-n} + \ldots + b_n \cdot (\prod_{i=0}^{n-1}(n-i)).$$

(Check this for your own!) By our first observation, this polynomial has order $\geq T$ at α if

$$L_n(b_0, \dots, b_L) := \sum_{j=n}^{L} b_j (\prod_{i=0}^{n-1}(j-i))\alpha^{j-n} = 0 \quad \forall\, n \in \{0, \dots, T-1\}. \tag{2.28}$$

Note that the L_n's are linear in the b_j's. So, we have T linear equations in $L+1$ variables, and by assumption we know $L + 1 > Td$. Hence, in order to apply Siegel's Lemma, we estimate the height of the linear equations $L_n \in \mathbb{Q}(\alpha)[x_1, \dots, x_{L+1}]$.

If $v \in M_{\mathbb{Q}(\alpha)}$ is non-archimedean, then we have (since once more the absolute value v of each integer is at most 1) for all $n \in \{0, \ldots, T-1\}$

$$|L_n|_v = \max_{n \le j \le L} \left| (\prod_{i=0}^{n-1} (j-i)) \alpha^{j-n} \right|_v \le \max_{n \le j \le L} \left| \alpha^{j-n} \right|_v = \max\{1, \left| \alpha^{L-n} \right|_v\}.$$

If $v \in M_{\mathbb{Q}(\alpha)}$ is archimedean, then we calculate for all $n \in \{0, \ldots, T-1\}$

$$|L_n|_v = \max_{n \le j \le L} \left| (\prod_{i=0}^{n-1} (j-i)) \alpha^{j-n} \right|_v \le \left| \prod_{i=0}^{n-1} (L-i) \right|_v \cdot \max\{1, \left| \alpha^{L-n} \right|_v\}.$$

We conclude that for all $n \in \{0, \ldots, T-1\}$ we have

$$\begin{aligned} H(L_n) &= \left(\prod_{v \in M_{\mathbb{Q}(\alpha)}} \max\{1, |L_n|_v^{d_v}\} \right)^{1/[\mathbb{Q}(\alpha):\mathbb{Q}]} \\ &\le \left(\prod_{\substack{v \in M_{\mathbb{Q}(\alpha)} \\ v|\infty}} \left| \prod_{i=0}^{n-1} (L-i) \right|_v^{d_v} \right)^{1/[\mathbb{Q}(\alpha):\mathbb{Q}]} \cdot \left(\prod_{v \in M_{\mathbb{Q}(\alpha)}} \max\{1, \left| \alpha^{L-n} \right|_v\}^{d_v} \right)^{1/[\mathbb{Q}(\alpha):\mathbb{Q}]} \\ &= \left(\prod_{i=0}^{n-1} (L-i) \right) \cdot \underbrace{H(\alpha^{L-n})}_{=H(\alpha)^{L-n}} < L^{T-1} H(\alpha)^L \end{aligned}$$

Now Siegel's Lemma guarantees that there are $b_0, \ldots, b_L \in \mathbb{Z}$ of absolute value at most

$$\left((L+1) L^{T-1} H(\alpha)^L \right)^{dT/L+1-dT},$$

not all equal to zero, satisfying all equations from (2.28). Conclusively, the polynomial $P(x) = b_L x^L + \ldots + b_0$ has $\mathrm{ord}_P(\alpha) \ge T$, $\deg(P) \le L$, and $H(P) \le \left((L+1) L^{T-1} H(\alpha)^L \right)^{dT/L+1-dT}$. □

For the proof of Roth's theorem, we need an extension of this result to polynomials in several variables. Before we take the effort to formulate and prove such an extension, we should present a convincing example, why statements like Proposition 2.4.11 are indeed helpful. This will be done in the next section. After that, we will handle the multi-variable case of this proposition. If you think that all of this is interesting enough without any example, you may want to read Section 2.6 before Section 2.5.

Exercises

Exercise 2.14. Prove Corollary 2.4.7.

Exercise 2.15. Find small integers x, y, z, not all zero, such that

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Exercise 2.16. Let F be a field and let $\overline{F}$ be an algebraic closure of F. For each $\alpha \in \overline{F}$ we extend the map

$$\mathrm{ord} : F[x] \setminus \{0\} \longrightarrow \mathbb{Z} \quad ; \quad f \mapsto \mathrm{ord}_f(\alpha)$$

to a map from the field of fractions $F(x)$ of $F[x]$, by setting $\mathrm{ord}_0(\alpha) = \infty$, and $\mathrm{ord}_{f/g}(\alpha) = \mathrm{ord}_f(\alpha) - \mathrm{ord}_g(\alpha)$ for all $f, g \in F[x] \setminus \{0\}$. Fix any real number $\varepsilon \in (0,1)$. Prove that $|\phi|_\alpha = \varepsilon^{\mathrm{ord}_\phi(\alpha)}$ is a non-archimedean absolute value on $F(x)$.
Here we use the rule $\varepsilon^\infty = 0$ for $\varepsilon \in (0,1)$.

2.5 On Lehmer's Conjecture

Denote the set of all roots of unity by μ. Recall that the Lehmer conjecture predicts a constant $c' > 0$ such that $M(\alpha) \geq 1 + c'$ for all $\alpha \in \overline{\mathbb{Q}}^* \setminus \mu$. If we formulate this in terms of the logarithmic height, the conjecture predicts a positive constant $c > 0$ such that $h(\alpha) \geq \frac{c}{d}$ for all algebraic numbers $\alpha \in \overline{\mathbb{Q}}^* \setminus \mu$ of degree d.
So we can measure the logarithmic height of an algebraic number asymptotically in its degree. The example

$$h(\sqrt[2]{2}) = \frac{\log(2)}{2}, \quad h(\sqrt[3]{2}) = \frac{\log(2)}{3}, \quad h(\sqrt[4]{2}) = \frac{\log(2)}{4}, \quad h(\sqrt[5]{2}) = \frac{\log(2)}{5}, \quad \ldots$$

shows that we cannot hope for a stronger bound than $h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]}$. Lehmer's conjecture is true for some classes of algebraic numbers. All of us know that it is true for all algebraic numbers, which are not an algebraic unit. This can be improved further: It is true for all algebraic numbers α, except for those which are algebraic units and Galois-conjugated to α^{-1} or $-\alpha^{-1}$.[4]
In Exercise 2.5 you have shown that it is true for all algebraic numbers, whose minimal polynomial has "large" discriminant. Moreover, in the optional Exercises 2.2 and 2.13 you can prove that it is true for all algebraic numbers, such that all Galois conjugates lie in a fixed completion of $\mathbb{Q}$.
The goal for this section is to prove the following theorem.

Theorem 2.5.1 (Dobrowolski)**.** *For all $\varepsilon > 0$ there is a constant $c(\varepsilon)$ such that*

$$h(\alpha) \geq \frac{c(\varepsilon)}{[\mathbb{Q}(\alpha) : \mathbb{Q}]^{1+\varepsilon}} \quad \text{for all } \alpha \in \overline{\mathbb{Q}}^* \setminus \mu.$$

So we are only an ε away from Lehmer's conjecture. However, this seems to be a very large step. Taking more care in the correct choices of parameters below, one can obtain a slightly stronger result, with which I will not bother you. We follow in this section the exhibition from [8].

Remark 2.5.2. In proving Theorem 2.5.1, it is enough to consider algebraic numbers α, with $h(\alpha) < \frac{\log(2)}{[\mathbb{Q}(\alpha):\mathbb{Q}]}$, since all the others satisfy a stronger inequality. In the exercises you have proved that $\log(2) \leq \log(M(\alpha)) = [\mathbb{Q}(\alpha) : \mathbb{Q}]h(\alpha)$ for all α which are not an unit in the ring of algebraic integers. Hence, we could assume throughout that α is an algebraic unit, different from a root of unity.

[4] We will not give further details. Everything can be found in [1].

Moreover, by Northcott's theorem 2.3.8 there are only finitely many numbers of bounded degree and bounded height. The height of these finitely many numbers, which are different from roots of unity, is surely bounded away from zero. Hence, it suffices to prove the bound in Theorem 2.5.1 for all algebraic numbers of huge degree, where this "huge" must depend on ε.

Now we set the agenda for the proof of Theorem 2.5.1.

Lemma 2.5.3. *Let T and L be positive integers, and let $\alpha \in \overline{\mathbb{Q}}$ be of degree d. If there is a prime number p, and a polynomial $P \in \mathbb{Z}[x]$ such that*

(i) $\deg(P) \leq L$,

(ii) $\mathrm{ord}_P(\alpha) \geq T$, *and*

(iii) $P(\alpha^p) \neq 0$.

Then we have

$$h(\alpha) \geq \frac{1}{pL} \cdot \log\left(\frac{p^T}{(L+1)\cdot H(P)}\right).$$

Proof. We assume that all assumptions of the lemma are met. Moreover, let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$ be the minimal polynomial of α. We reduce f modulo p. That is we apply the canonical projection

$$\pi : \mathbb{Z}[x] \longrightarrow \mathbb{F}_p[x].$$

Since $\mathbb{F}_p$ has characteristic p, it is well known[5] that $z \mapsto z^p$ is a homomorphism on $\mathbb{F}_p[x]$. Combining this with Fermat's little theorem ($z^p \equiv z \mod p$ for all $z \in \mathbb{F}_p$), we achieve $\pi(f(x)^p) = \pi(f(x^p))$. Hence, there is a polynomial $g \in \mathbb{Z}[x]$ such that

$$f(x^p) = f(x)^p + pg(x) \qquad \text{and} \qquad \deg(g) \leq d \cdot p. \tag{2.29}$$

The latter statement comes simply from comparing the degrees. It is $\deg(f(x)^p) = d \cdot p = \deg(f(x^p))$. Hence, the degree of g cannot be larger than $d \cdot p$.
We know that $\mathrm{ord}_P(\alpha) \geq T$ and hence α is a root of P of multiplicity at least T. This means that $f(x)$ divides $P(x)$ at least T-times. Therefore, there is a $q(x) \in \mathbb{Z}[x]$ such that $f(x)^T \cdot q(x) = P(x)$, and $\deg(q) = \deg(P) - \deg(f^T) \leq L - dT$. We combine this with (2.29), which yields

$$P(x^p) = f(x^p)^T q(x^p) = (f(x)^p + pg(x))^T \cdot q(x^p).$$

We plug in α and define its image as

$$\beta = P(\alpha^p) = (\underbrace{f(\alpha)^p}_{=0} + pg(\alpha))^T \cdot q(\alpha^p) = p^T g(\alpha)^T \cdot q(\alpha^p).$$

The degree of $g(x)^T \cdot q(x^p)$ is at most $Tdp + p(L - dT) = pL$. Therefore

$$g(\alpha)^T \cdot q(\alpha^p) = b_{pL}\alpha^{pL} + b_{pL}\alpha^{pL-1} + \ldots b_0 \text{ , with } b_0, \ldots, b_{pL} \in \mathbb{Z}.$$

[5] This phrase should be a red flag for you! It just means that I assume you know this result, and I am to lazy to explain it further.

Let K be any number field containing α, and let $v \in M_K$ be arbitrary. If v is non-archimedean, the ultrametric inequality (and the fact $|b_i|_v \leq 1$ for all $i \in \{1, \dots, b_{pL}\}$) implies

$$|\beta|_v = \left|p^T g(\alpha)^T \cdot q(\alpha^p)\right|_v = |p|_v^T \left|g(\alpha)^T \cdot q(\alpha^p)\right|_v \leq |p|_v^T \max\{1, |\alpha|_v\}^{pL}.$$

We want to bound the height of α in terms of p. Hence, we will not apply the usual estimate $|p|_v \leq 1$, which would remove the p. Actually, doing so would give a trivial (negative) bound for the logarithmic height of α. If v is archimedean, then

$$|\beta|_v = |P(\alpha^p)|_v \leq \underbrace{(\deg(P)+1)}_{\text{number of coeff. of } P} H(P) \max\{1, |\alpha|_v\}^{p \deg(P)} \leq (L+1) H(P) \max\{1, |\alpha|_v\}^{pL}.$$

By assumption, $\beta = P(\alpha^p) \neq 0$. Hence, the product formula 2.2.16 gives

$$\begin{aligned} 1 &= \prod_{v \in M_K} |\beta|_v^{d_v} \\ &\leq \prod_{v \in M_K, v \nmid \infty} |p|_v^{d_v T} \cdot \prod_{v \in M_K, v \mid \infty} ((L+1)H(P))^{d_v} \cdot \prod_{v \in M_K} \max\{1, |\alpha|_v^{pL}\}^{d_v} \\ &= p^{-T[K:\mathbb{Q}]} ((L+1)H(P))^{[K:\mathbb{Q}]} H(\alpha)^{Lp[K:\mathbb{Q}]}. \end{aligned}$$

A tiny bit of algebra transfers this inequality into

$$H(\alpha) \geq \left(\frac{p^T}{(L+1)H(P)}\right)^{\frac{1}{pL}}.$$

Taking logarithms now proves the lemma. □

In order to prove Theorem 2.5.1, we will prove the existence of a prime p and a polynomial P satisfying the assumptions in Lemma 2.5.3, such that the claimed height bound drops out. It should not surprise you, that the existence of the polynomial P follows from Siegel's Lemma 2.4.6. More precisely, we will use the polynomial P from Proposition 2.4.11. This $P \in \mathbb{Z}[x]$ already satisfies two of the three assumptions from Lemma 2.5.3. To ensure $P(\alpha^p) \neq 0$ for some "nice" prime number p, we need a bit of Algebra and (of course) the prime number theorem.

Lemma 2.5.4. *Let $\alpha \in \overline{\mathbb{Q}}$ be arbitrary of degree d. Then there are at most $\frac{\log(d)}{\log(2)}$ prime numbers p such that $[\mathbb{Q}(\alpha^p) : \mathbb{Q}] \neq d$.*

Proof. Let $p_1, \dots, p_n$ be distinct primes such that $[\mathbb{Q}(\alpha^{p_i}) : \mathbb{Q}] < d$ for all $i \in \{1, \dots, n\}$. This is, $\alpha \notin \mathbb{Q}(\alpha^{p_i})$ for all $i \in \{1, \dots, n\}$. We define $K_0 = \mathbb{Q}(\alpha)$ and for all $i \in \{1, \dots, n\}$ we set $K_i = \mathbb{Q}(\alpha^{p_1 \cdots p_i})$. Then we have a chain of number fields

$$\mathbb{Q} \subseteq K_n \subseteq K_{n-1} \subseteq \dots \subseteq K_1 \subseteq K_0 = \mathbb{Q}(\alpha). \tag{2.30}$$

We claim that for each $i \in \{1, \dots, n\}$ we have $K_i \neq K_{i-1}$. Assume that $K_i = K_{i-1}$ for some $i \in \{1, \dots, n\}$. Then $\alpha^{p_1 \cdots p_{i-1}} \in \mathbb{Q}(\alpha^{p_i \cdot (p_1 \cdots p_{i-1})}) \subseteq \mathbb{Q}(\alpha^{p_i})$. However, by Bézout's lemma there are $u, v \in \mathbb{Z}$ such that $1 = p_i u + (p_1 \cdots p_{i-1}) v$. Hence,

$$\alpha = \alpha^1 = \alpha^{p_i u + (p_1 \cdots p_{i-1})v} = \underbrace{(\alpha^{p_i})^u}_{\in \mathbb{Q}(\alpha^{p_i})} \cdot \underbrace{(\alpha^{p_1 \cdots p_{i-1}})^v}_{\in \mathbb{Q}(\alpha^{p_i})} \in \mathbb{Q}(\alpha^{p_i}).$$

But this implies $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^{p_i})$, contradicting the main property of p_i. Hence – as claimed – all inclusions in (2.30) are strict. In particular,

$$d = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \underbrace{[K_0 : K_1]}_{\geq 2} \cdot \underbrace{[K_1 : K_2]}_{\geq 2} \cdot \ldots \cdot \underbrace{[K_{n-1} : K_n]}_{\geq 2} \cdot [K_n : \mathbb{Q}] \geq 2^n.$$

Hence $n \leq \frac{\log(d)}{\log(2)}$, as proposed. □

Theorem 2.5.5 (Prime Number Theorem)**.** *Denote for any $x \in \mathbb{R}$ the number of prime numbers less or equal to x by $\pi(x)$. Then*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log(x)} = 1.$$

For our purposes a much weaker result would suffice. We only need that for large x there are many prime numbers between x and $2x$. For instance we could use Ramanujan's version of Bertrand's postulate [13]: For all $x > 0$ we have $\pi(2x) - \pi(x) > \frac{1}{\log(2x)} \cdot (\frac{1}{3}x - 3\sqrt{2x})$, which surely tends to infinity for increasing x. We conclude a similar statement ineffectively from the prime number theorem:

Corollary 2.5.6. *Let $\delta, c, \chi > 0$ be given positive constants. Then there is a constant $\kappa(\delta, c, \chi)$, such that for all $d \geq \kappa(\delta, c, \chi)$, there are more than $\chi + \log(d)/\log(2)$ prime numbers between cd^δ and $2cd^\delta$.*

Proof. With $\pi(x)$ as above, the prime number theorem 2.5.5 gives $\lim_{x\to\infty} \frac{\pi(2x)-\pi(x)}{x/\log(x)} = 1$. This is, there are asymptotically $x/\log(x)$ primes between x and $2x$. Hence, there are asymptotically $cd^\delta/\log(cd^\delta)$ primes between cd^δ and $2cd^\delta$, for increasing d. The statement of the corollary follows by noting

$$\frac{cd^\delta}{\log(cd^\delta)} - \frac{\log(d)}{\log(2)} \longrightarrow \infty \quad \text{as } d \to \infty.$$

"d to the power of a positive whatsoever grows faster than $\log(d)$." □

Proof of Theorem 2.5.1. We want to prove that for all $\varepsilon > 0$ there exists a constant $c(\varepsilon)$ such that $h(\alpha) \geq \frac{c(\varepsilon)}{[\mathbb{Q}(\alpha):\mathbb{Q}]}$ for all $\alpha \in \overline{\mathbb{Q}}^* \setminus \mu$, where μ is the set of roots of unity.
We should start by fixing an $\varepsilon > 0$. We already have outlined the proof. We will fix some parameters L and T (depending on ε), and then we will apply Lemma 2.5.3 for a polynomial constructed by Proposition 2.4.11, and a "nice" prime number p which exists by Lemma 2.5.4 and Corollary 2.5.6.
We make the following choices:

(A) Let $\alpha \in \overline{\mathbb{Q}}^* \setminus \mu$ be of degree d, such that $M(\alpha) = H(\alpha)^d \leq 2$. As noted already in Remark 2.5.2, this restriction does not jeopardize the conclusion of the theorem.

(B) Let $T \in \mathbb{N}$ be such that $\frac{1}{T} < \varepsilon$.

(C) Set $\chi \in \mathbb{R}$ such that $\varepsilon = \frac{1}{T} + \frac{T}{\chi - T}$. From (B) it follows that $\chi > T$.

(D) Set $L = \lfloor \chi d \rfloor$.

With these choices we run our agenda[6]. By Proposition 2.4.11 there is a polynomial $P \in \mathbb{Z}[x]$ of degree at most L, $\mathrm{ord}_P(\alpha) \geq T$, and

$$\begin{aligned} H(P) &\leq \left((L+1)L^{T-1}H(\alpha)^L\right)^{\frac{dT}{L+1-dT}} \overset{(A)}{\leq} \left((L+1)L^{T-1}\right)^{\frac{dT}{L+1-dT}} \cdot 2^{\frac{LT}{L+1-dT}} \\ &\overset{(D)}{\leq} \left((L+1)L^{T-1}\right)^{\frac{T}{\chi-T}} \cdot 2^{\frac{\chi T}{\chi-T}} \leq (2L)^{\frac{T^2}{\chi-T}} \cdot 2^{\frac{\chi T}{\chi-T}} \\ &\overset{(D)}{\leq} (2\chi d)^{\frac{T^2}{\chi-T}} 2^{\frac{\chi T}{\chi-T}} = \left((2\chi)^{\frac{T^2}{\chi-T}} 2^{\frac{\chi T}{\chi-T}}\right) \cdot d^{\frac{T^2}{\chi-T}}. \end{aligned} \tag{2.31}$$

Keeping Lemma 2.5.3 in mind, we need a prime number p which is not too big, but greater than

$$(L+1) \cdot H(P) \overset{(D)}{\leq} (2\chi d)H(P) \overset{(2.31)}{\leq} C(T,\chi)d^{1+\frac{T^2}{\chi-T}}, \tag{2.32}$$

where $C(T,\chi) = 2\chi\left((2\chi)^{\frac{T^2}{\chi-T}}2^{\frac{\chi T}{\chi-T}}\right)$ only depends on T, and χ. In particular $C(T,\chi)$ is independent on the degree d. By Corollary 2.5.6 (with $\delta = \varepsilon = \frac{1}{T} + \frac{T}{\chi-T}$ and $c = \sqrt[T]{2C(\chi,T)}$), there are more than $\chi + \log(d)/\log(2)$ primes p such that

$$2C(T,\chi)d^{1+\frac{T^2}{\chi-T}} \leq p^T \leq 2^{T+1}C(T,\chi)d^{1+\frac{T^2}{\chi-T}}, \tag{2.33}$$

whenever $d \geq \kappa(T,\chi)$, for some constant only depending on T and χ.

(E) From now on we assume that we have $d \geq \kappa(T,\chi)$.

Among all the prime numbers satisfying (2.33), by Lemma 2.5.4 there are different prime numbers $p_1, \ldots, p_n$, with $n \geq \chi + 1$ such that $[\mathbb{Q}(\alpha^{p_i}) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ for all $i \in \{1, \ldots, n\}$. Since α is not a root of unity, α^p and α^q are not Galois conjugated for different primes p and q (cf. Exercise 2.12). Therefore, all the minimal polynomials of $\alpha^{p_1}, \ldots, \alpha^{p_n}$ are distinct. Hence, if $P(\alpha^{p_i}) = 0$ for all $i \in \{1, \ldots, n\}$, then all these n minimal polynomials of degree d divide P. But then the degree of P would be at least $d \cdot n \geq d(\chi+1) \overset{(D)}{>} L \geq \deg(P)$, which is a contradiction.

(F) Hence, there is (at least) one prime p satisfying (2.33) such that $P(\alpha^p) \neq 0$.

Now we have all ingredients to finally apply Lemma 2.5.3. This gives

$$\begin{aligned} h(\alpha) &\geq \frac{1}{pL} \cdot \log\left(\frac{p^T}{(L+1)\cdot H(P)}\right) \overset{(2.32)}{\geq} \frac{1}{pL} \cdot \log\left(\frac{p^T}{C(T,\chi)d^{1+T^2/\chi-T}}\right) \\ &\overset{(2.33)}{\geq} \frac{1}{pL} \cdot \log(2) \overset{(2.33),(D)}{\geq} \frac{1}{2^{T+1/T}C(T,\chi)^{1/T}d^{1/T+\frac{T}{\chi-T}}\chi d} \log(2) \overset{(C)}{=} C_2(\chi,T) \cdot \frac{1}{d^{1+\varepsilon}}, \end{aligned}$$

where $C_2(\chi,T) = \frac{\log(2)}{2^{T+1/T}C(T,\chi)^{1/T}\chi}$ only depends on T and χ, but is independent on d. Since T and χ depend on ε, this is precisely what we wanted to prove. But recall that this bound

[6] If one proves the Theorem for the first time, one has to work with undetermined values for L and T. Then, at the end of the proof, one can fix L and T that satisfy all assumptions one had to apply. That we can work with these magically appearing constants, is due to the fact that it is not the first time that someone proves this theorem.

is only valid for α such that $M(\alpha) = H(\alpha)^d \leq 2$ (by (A)), and $[\mathbb{Q}(\alpha) : \mathbb{Q}] \geq \kappa(T, \chi)$ (by (E)). But by Northcott's theorem 2.1.8, there are only finitely many α of degree $\leq \kappa(T, \chi)$ and $M(\alpha) \leq 2$. Let c be the smallest positive value of the logarithmic height of these finitely many numbers, then

$$h(\alpha) \geq \min\{c, 2, C_2(T, \chi)\} \cdot \frac{1}{d^{1+\varepsilon}} \quad \forall\, \alpha \in \overline{\mathbb{Q}}^* \setminus \mu.$$

Hence, with any choice of T, χ satisfying (B) and (C), we can conclude Theorem 2.5.1. □

Remark 2.5.7. If you take the trouble to go through the proof once more, you will notice, that the constant $c(\varepsilon)$ in Theorem 2.5.1 can be explicitly determined. So the result is fully effective.

Remark 2.5.8. Let us recall the basic steps of the proof. We wanted to prove something about a given $\alpha \in \overline{\mathbb{Q}}$. We used a particular polynomial, which vanished at α (we called this P). This polynomial was not allowed to vanish at a certain other number α^p. Moreover, it was necessary to estimate the "size" of $P(\alpha^p)$ (see the β in the proof of Lemma 2.5.3). Comparing α and $P(\alpha^p)$ gave the result we were longing for.
Stated this way, you may notice a similarity to the very first proof of Liouville's Theorem 1.1.12. There, the polynomial was just the minimal polynomial f of α. The second number was a rational $\frac{p}{q}$, and it was obvious that f did not vanish at this rational number. Also the "size" of $f(\frac{p}{q})$ was easily determined. Comparing α and $f(\frac{p}{q})$ concluded the proof.
Undoubtedly the proof of Dobrowolski's Theorem 2.5.1 was much more advanced than the simple proof of Liouville's Theorem 1.1.12. But (taking the right perspective) the skeletons of both proofs share some strong similarities. The basic parts outlined above, will also be visible in the skeleton of the proof of Roth's theorem! But again we have lift things to the next level of complexity.

Remark 2.5.9. Very recently (a few month ago), the little brother of Lehmer's conjecture – the Schinzel-Zassenhaus conjecture – has been proved by Vesselin Dimitrov [4]: For any non-cyclotomic monic irreducible polynomial $f(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_d) \in \mathbb{Z}[x]$, we have

$$\max_{1 \leq i \leq d} |\alpha_i| \geq 2^{\frac{1}{4d}}.$$

Exercises

Exercise 2.17. Proof that Lehmer's conjecture implies the existence of a constant $c > 1$, such that $\max_{1 \leq i \leq d} |\alpha_i| \geq c^{\frac{1}{d}}$ for all monic non-cyclotomic irreducible polynomials $f(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_d) \in \mathbb{Z}[x] \setminus \{x\}$ of degree at least 1.

Exercise 2.18. Find explicit positive constants $c, \kappa \in \mathbb{R}$ such that $h(\alpha) \geq \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]^{1+\frac{1}{2}}}$ for all $\alpha \in \overline{\mathbb{Q}}^* \setminus \mu$ of degree $\geq \kappa$.

2.6 Siegel's Lemma Once More

In the last section we saw that an auxiliary polynomial, constructed by the aid of Siegel's lemma, can be a helpful tool. As stated before, in order to prove Roth's theorem, we need an

Or, rephrasing this, the order of P at α is given by the minimal T such that the Tth derivative of P does not vanish at α.

Proposition 2.4.10. *Let $\alpha \in \overline{\mathbb{Q}}$ be arbitrary of degree d, and let T and L be positive integers, with $L \geq dT$. Then there exists a polynomial $P \in \mathbb{Z}[x] \setminus \{0\}$, such that*

(i) $\deg(P) \leq L$,

(ii) $\mathrm{ord}_P(\alpha) \geq T$, *and*

(iii) $H(P) \leq \left((L+1)L^{T-1}H(\alpha)^L\right)^{dT/L+1-dT}$.

auxiliary polynomial in multiple variables. Hence, we are going to formulate a multi-variable version of Proposition 2.4.11, which stated:
Of course we know how to measure the degree of a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_n]$. We will work with the partial degrees in each variable. This is, for each $i \in \{1, \ldots, n\}$, the *degree at* x_i of P, is the degree of P considered as a polynomial in $(\mathbb{Z}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n])[x_i]$, and we denote it by $\deg_{x_i}(P)$.
The height of a polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$ is also already defined: It is simply the maximum of all absolute values of its coefficients. Hence, it remains to generalize the order of P at a given point. This will surely be linked to the derivatives of P. For every $\underline{d} = (d_1, \ldots, d_n) \in \mathbb{N}_0^n$ the operator

$$\frac{\partial^{\underline{d}}}{\partial \underline{x}^{\underline{d}}} P = \frac{\partial^{d_1}}{\partial x_1^{d_1}} \frac{\partial^{d_2}}{\partial x_2^{d_2}} \cdots \frac{\partial^{d_n}}{\partial x_n^{d_n}} P$$

takes the d_1th partial derivative of P at x_1, then the d_2th partial derivative of P at x_2, and so on. We know from slightly after elementary school that this is independent on the order in which one takes the partial derivatives.

Lemma 2.6.1. *For any $\underline{d} = (d_1, \ldots, d_n) \in \mathbb{N}_0^n$, and any $P \in \mathbb{Z}[x_1, \ldots, x_n]$, each coefficient of $\frac{\partial^{\underline{d}}}{\partial \underline{x}^{\underline{d}}} P$ is divisible by $d_1! \cdot \ldots \cdot d_n!$.*

Proof. The main part has already been done, since we know this result for a single variable. Taking the dth derivative of the monomial x^k yields (cf. the proof of Proposition 2.4.11)

$$\frac{\partial^d}{\partial x^d} x^k = k \cdot (k-1) \cdot \ldots \cdot (k-d+1) x^{k-d} = d! \binom{k}{d} x^{k-d},$$

where the latter equation is just applying the well-known formula for the binomial coefficient, with the usual extra that $\binom{k}{d} = 0$ whenever $d > k$. Let $P = \sum_{\underline{i} \in \mathbb{N}_0^n} c_{\underline{i}} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n} \in \mathbb{Z}[x_1, \ldots, x_n]$ be arbitrary (we still use $\underline{i} = (i_1, \ldots, i_n)$). Then

$$\begin{aligned}
\frac{\partial^{\underline{d}}}{\partial \underline{x}^{\underline{d}}} P &= \sum_{\underline{i} \in \mathbb{N}_0^n} c_{\underline{i}} \frac{\partial^{\underline{d}}}{\partial \underline{x}^{\underline{d}}} x_1^{i_1} \cdots x_n^{i_n} = \sum_{\underline{i} \in \mathbb{N}_0^n} c_{\underline{i}} \left(\frac{\partial^{d_1}}{\partial x_1^{d_1}} x_1^{i_1} \right) \cdots \left(\frac{\partial^{d_n}}{\partial x_n^{d_n}} x_n^{i_n} \right) \\
&= \sum_{\underline{i} \in \mathbb{N}_0^n} c_{\underline{i}} \left(d_1! \binom{i_1}{d_1} x_1^{i_1 - d_1} \right) \cdots \left(d_n! \binom{i_n}{d_n} x_n^{i_n - d_n} \right) \\
&= (d_1! \cdots d_n!) \cdot \underbrace{\sum_{\underline{i} \in \mathbb{N}_0^n} c_{\underline{i}} \binom{i_1}{d_1} \cdots \binom{i_n}{d_n} x_1^{i_1 - d_1} \cdots x_n^{i_n - d_n}}_{\in \mathbb{Z}[x_1, \ldots, x_n]}, \qquad (2.34)
\end{aligned}$$

which proves the claim. □

We want to achieve a polynomial with small integral coefficients. Hence, we will work from now on with the following normalization of the derivative of $P \in \mathbb{Z}[x_1, \ldots, x_n]$. For each $\underline{d} = (d_1, \ldots, d_n) \in \mathbb{N}_0^n$ we set

$$\partial_{\underline{d}} P = \frac{1}{d_1! \cdots d_n!} \cdot \frac{\partial^{\underline{d}}}{\partial \underline{x}^{\underline{d}}} P \overset{2.6.1}{\in} \mathbb{Z}[x_1, \ldots, x_n].$$

Note that (2.34) gives a precise formula for this normalized derivative!
Now we can generalize the order of a polynomial. Again, we have to make things slightly more complicated, and add another normalization.

Definition 2.6.2. For points $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$, and $\underline{r} = (r_1, \ldots, r_n) \in \mathbb{N}^n$, we define for all $P \in \mathbb{C}[x_1, \ldots, x_n] \setminus \{0\}$ the *index of P with respect to $\underline{\alpha}$ and $\underline{r}$* to be

$$\mathrm{Ind}_{(\underline{\alpha},\underline{r})}(P) = \min\{\frac{i_1}{r_1} + \ldots + \frac{i_n}{r_n} | (i_1, \ldots, i_n) \in \mathbb{N}_0^n \text{ and } \partial_{(i_1,\ldots,i_n)} P(\underline{\alpha}) \neq 0\}.$$

Hence, the index of a polynomial at $\underline{\alpha}$ is up to normalization the smallest value $i_1 + \ldots + i_n$, such that the $(i_1, \ldots, i_n)$th derivative does not vanish at $\underline{\alpha}$.

Example 2.6.3.

- Let $k \geq q \geq 1$ and $P(x, y) = x^k - y^q \in \mathbb{C}[x, y]$. Then

  $$\mathrm{Ind}_{((0,0),(k,k))}(P) = \frac{q}{k},$$

  since $\partial_{(i,j)} P(0, 0) = 0$, whenever $i < k$ and $j < q$. On the other hand $\partial_{(0,q)} P = -q!\binom{q}{q} y^0 = -q!$, does not vanish at $(0, 0)$.

- We have $\mathrm{Ind}_{(\underline{\alpha},\underline{r})}(P) = 0$ if and only if the $(0, \ldots, 0)$th derivative of P does not vanish at $\underline{\alpha}$. This means, that the index is zero if and only if $P(\underline{\alpha}) \neq 0$.

- Let $P \in \mathbb{C}[x_1, \ldots, x_n] \setminus \{0\}$ be arbitrary, and choose integers $i_1, \ldots, i_n \in \mathbb{N}_0$, such that $i_k > \deg_{x_k}(P)$ for at least one $k \in \{1, \ldots, n\}$. Then $\partial_{(i_1,\ldots,i_n)} P = 0$. Hence, if $\partial_{(i_1,\ldots,i_n)} P \neq 0$ we have $i_k \leq \deg_{x_k}(P)$ for all $k \in \{1, \ldots, n\}$. In particular, for all $\underline{\alpha} \in \mathbb{C}^n$ and all $\underline{r} = (r_1, \ldots, r_n) \in \mathbb{N}^n$, we have the estimate

  $$\mathrm{Ind}_{(\underline{\alpha},\underline{r})}(P) \leq \sum_{i=1}^{n} \frac{\deg_{x_i}(P)}{r_i}.$$

  Thus, the index is indeed a well defined rational number.

Finally, we have all ingredients at hand to formulate a generalization of Proposition 2.4.11. However, for the proof we need one more lemma.

Lemma 2.6.4. *Let $(r_1, \ldots, r_n) \in \mathbb{N}^n$ and $\varepsilon \in (0, 1)$. Then there are at most*

$$(r_1 + 1) \cdots (r_n + 1) \cdot e^{-\varepsilon^2 n/4}$$

elements $(d_1, \ldots, d_n) \in \{0, \ldots, r_1\} \times \ldots \times \{0, \ldots, r_n\}$ such that $\sum_{i=1}^n \frac{d_i}{r_i} \leq \frac{n}{2}(1 - \varepsilon)$.

Proof. We do not present every single detail of the proof. Set $B(r_1,\dots,r_n)$ to be the "box" $\{0,\dots,r_1\}\times\ldots\times\{0,\dots,r_n\}$. We need to estimate the cardinality of

$$I(n,\varepsilon)=\{(d_1,\dots,d_n)\in B(r_1,\dots,r_n)|\sum_{i=1}^{n}\frac{d_i}{r_i}\leq\frac{n}{2}(1-\varepsilon)\}.$$

By definition, each $(d_1,\dots,d_n)\in I(n,\varepsilon)$ satisfies $\exp(\frac{n}{2}-\frac{\varepsilon n}{2}-\sum_{i=1}^{n}\frac{d_i}{r_i})\geq 1$. Moreover, $\exp(\frac{n}{2}-\frac{\varepsilon n}{2}-\sum_{i=1}^{n}\frac{d_i}{r_i})>0$ for any $(d_1,\dots,d_n)\in\mathbb{N}_0^n$ (simply, since e^t is always positive). Of course, we can multiply the term inside the exp(.) by any positive real number, without changing these estimates. Hence, we have

$$\begin{aligned}|I(n,\varepsilon)|&=\sum_{\underline{d}\in I(n,\varepsilon)}1\leq\sum_{\underline{d}\in B(r_1,\dots,r_n)}\exp\left(\varepsilon\left(\frac{n}{2}-\frac{\varepsilon n}{2}-\sum_{i=1}^{n}\frac{d_i}{r_i}\right)\right)\\&=\exp\left(-\frac{\varepsilon^2 n}{2}\right)\prod_{h=1}^{n}\left(\sum_{i=0}^{r_h}\exp\left(\varepsilon\left(\frac{1}{2}-\frac{i}{r_h}\right)\right)\right)\end{aligned}\tag{2.35}$$

The summand $\varepsilon\left(\frac{1}{2}-\frac{i}{r_h}\right)$ always lies in $(-\varepsilon/2,\varepsilon/2)\subseteq(-1,1)$. Using the inequality $\exp(t)\leq 1+t+t^2$ for all $t\in(-1,1)$, one shows

$$\sum_{i=0}^{r_h}\exp\left(\varepsilon\left(\frac{1}{2}-\frac{i}{r_h}\right)\right)\leq(r_h+1)(1+\varepsilon^2/4)\quad\forall\ h\in\{1,\dots,n\}.$$

Combining this estimate with (2.35), and applying $1+t\leq\exp t$ for all $t\in\mathbb{R}$, gives the claimed result. □

Finally we are willing and able to prove the generalization of Proposition 2.4.11.

Theorem 2.6.5. *Let $\alpha\in\overline{\mathbb{Q}}$ be of degree d. Moreover, let $\varepsilon\in(0,1)$ and $n\in\mathbb{N}$ such that $\exp(\varepsilon^2 n/4)\geq 2d$, and set $\underline{\alpha}=(\alpha,\dots,\alpha)\in\overline{\mathbb{Q}}^n$. For every $\underline{r}=(r_1,\dots,r_n)\in\mathbb{N}^n$ there exists a polynomial $P\in\mathbb{Z}[x_1,\dots,x_n]\setminus\{0\}$ such that*

(i) $\deg_{x_i}(P)\leq r_i$ *for all* $i\in\{1,\dots,n\}$,

(ii) $\mathrm{Ind}_{(\underline{\alpha},\underline{r})}(P)\geq\frac{n}{2}(1-\varepsilon)$, *and*

(iii) $H(P)\leq(4H(\alpha))^{r_1+\ldots+r_n}$.

Proof. Of course we want to apply Siegel's lemma. Hence, we need to find certain linear equations for the coefficients of P. We want that the degree of P at x_i is bounded by r_i for all $i\in\{1,\dots,n\}$. Hence, any monomial appearing in P with a non-zero coefficient, is of the form $x_1^{i_1}\cdots x_n^{i_n}$, with

$$(i_1,\dots,i_n)\in\{0,\dots,r_1\}\times\ldots\times\{0,\dots,r_n\}=:B(r_1,\dots,r_n).$$

Hence, we are looking for a polynomial

$$P(x_1,\dots,x_n)=\sum_{\underline{i}\in B(r_1,\dots,r_n)}c_{\underline{i}}x_1^{i_1}\cdots x_n^{i_n}\in\mathbb{Z}[x_1,\dots,x_n].$$

Such a polynomial has $N = |B(r_1, \dots, r_n)| = (r_1+1)\cdots(r_n+1)$ coefficients, which we handle as unknowns.
The bound in (ii) for the index of P is true, if and only if

$$\begin{aligned} 0 = \partial_{\underline{d}} P(\underline{\alpha}) &\overset{(2.34)}{=} \sum_{\underline{i}\in B(r_1,\dots,r_n)} c_{\underline{i}} \binom{i_1}{d_1}\cdots\binom{i_n}{d_n}\alpha^{i_1-d_1}\cdots\alpha^{i_n-d_n} \\ &= \sum_{\underline{i}\in B(r_1,\dots,r_n)} c_{\underline{i}} \binom{i_1}{d_1}\cdots\binom{i_n}{d_n}\alpha^{(i_1+\dots+i_n)-(d_1+\dots+d_n)} \end{aligned} \tag{2.36}$$

for all $\underline{d} = (d_1, \dots, d_n) \in \mathbb{N}^n$ such that $\sum_{i=1}^n \frac{d_i}{r_i} < \frac{n}{2}(1-\varepsilon)$. By Lemma 2.6.4 there are at most $|B(r_1, \dots, r_n)| \exp(-\varepsilon^2 n/4)$ of such tuples. Hence, our assumption on ε guarantees that the number of equations in 2.36 is

$$M \le N \cdot \exp(-\varepsilon^2 n/4) \le \frac{N}{2d}. \tag{2.37}$$

This enables us to apply Siegel's Lemma 2.4.6 to the M linear equations in N unknowns given in (2.36), which are defined over the number field $\mathbb{Q}(\alpha)$ of degree d.[7] It only remains to calculate the height of such an equation. Therefore, let $v \in M_{\mathbb{Q}(\alpha)}$ be archimedean, then

$$\begin{aligned} &\left|\binom{i_1}{d_1}\cdots\binom{i_n}{d_n}\alpha^{(i_1+\dots+i_n)-(d_1+\dots+d_n)}\right|_v \\ \le &\left|2^{i_1+\dots+i_n}\right|_v \cdot \max\{1, |\alpha|_v^{i_1+\dots+i_n}\} \le 2^{r_1+\dots+r_n} \cdot \max\{1, |\alpha|_v\}^{r_1+\dots+r_n}. \end{aligned} \tag{2.38}$$

Here we have used the generous estimate $\binom{i}{d} \le 2^i$, which is obvious from a combinatorial point of view: $\binom{i}{d}$ is the number of subsets of cardinality d of a set of cardinality i, and 2^i is the total number of subsets of a set of cardinality i.
Now let $v \in M_{\mathbb{Q}(\alpha)}$ be non-archimedean. Then

$$\begin{aligned} &\left|\binom{i_1}{d_1}\cdots\binom{i_n}{d_n}\alpha^{(i_1+\dots+i_n)-(d_1+\dots+d_n)}\right|_v \\ \le &\max\{1, |\alpha|_v^{i_1+\dots+i_n}\} \le \max\{1, |\alpha|_v\}^{r_1+\dots+r_n}. \end{aligned} \tag{2.39}$$

We can conclude that the multiplicative height of any of the polynomials in (2.36) (keep in mind that the $c_{\underline{i}}$'s are the unknowns) is less or equal to

$$\begin{aligned} &\prod_{\substack{v\in M_{\mathbb{Q}(\alpha)}\\ v|\infty}} \left(2^{r_1+\dots+r_n} \cdot \max\{1, |\alpha|_v\}^{r_1+\dots+r_n}\right)^{d_v/d} \cdot \prod_{\substack{v\in M_{\mathbb{Q}(\alpha)}\\ v\nmid\infty}} \left(\max\{1, |\alpha|_v\}^{r_1+\dots+r_n}\right)^{d_v/d} \\ = &\prod_{\substack{v\in M_{\mathbb{Q}(\alpha)}\\ v|\infty}} \left(2^{r_1+\dots+r_n}\right)^{d_v/d} \cdot \prod_{v\in M_{\mathbb{Q}(\alpha)}} \left(\max\{1, |\alpha|_v\}^{r_1+\dots+r_n}\right)^{d_v/d} \\ = &2^{r_1+\dots+r_n} H(\alpha)^{r_1+\dots+r_n} = (2H(\alpha))^{r_1+\dots+r_n}. \end{aligned}$$

[7] Actually it would be enough to assume $M \le N/d$ in order to apply Siegel's Lemma. The 2 is only included, so that we can bound the exponent appearing in Siegel's Lemma by 1 (see the second to last inequality in the proof).

We apply Siegel's Lemma 2.4.6, and conclude that there are coefficients $c_{\underline{i}} \in \mathbb{Z}$, such that all equations from (2.36) are satisfied, and such that

$$\begin{aligned} H\Big(\sum_{\underline{i}\in B(r_1,\dots,r_n)} c_{\underline{i}} x_1^{i_1}\cdots x_n^{i_n}\Big) &\le \Big(N(2H(\alpha))^{r_1+\dots+r_n}\Big)^{dM/(N-dM)} \\ &= \Big((r_1+1)\cdots(r_n+1)\cdot(2H(\alpha))^{r_1+\dots+r_n}\Big)^{\frac{1}{N/dM-1}} \\ &\overset{(2.37)}{\le} (r_1+1)\cdots(r_n+1)\cdot(2H(\alpha))^{r_1+\dots+r_n} \le (4H(\alpha))^{r_1+\dots+r_n}. \end{aligned}$$

The last inequality comes again from comparing binomial coefficients with a power of 2: we have $1+r = \binom{r}{0} + \binom{r}{1} \le 2^r$. This proves the theorem. □

Exercises

Exercise 2.19. Let $\underline{\alpha} \in \mathbb{C}^n$ and $\underline{r} \in \mathbb{N}^n$ be arbitrary. Prove that for all $P, P' \in \mathbb{C}[x_1,\dots,x_n]\setminus\{0\}$, we have

$$\mathrm{Ind}_{(\underline{\alpha},\underline{r})}(P\cdot P') = \mathrm{Ind}_{(\underline{\alpha},\underline{r})}(P) + \mathrm{Ind}_{(\underline{\alpha},\underline{r})}(P').$$

Chapter 3

Roth's Theorem

Roth's theorem is around since the very first lecture. It served as a motivation for introducing the Mahler measure and the height, although theses functions are – of course – of independent interest. Recall from (RT7):

Roth's Theorem 3.0.1. *Let K be a number field of degree d, and let $S \subseteq M_K$ be finite. For any $\alpha \in \overline{\mathbb{Q}}$ and for each element $v \in M_K$ we fix one extension $v' \mid v$ to $K(\alpha)$. Then, for all $\varepsilon > 0$ there are at most finitely many $\beta \in K$ such that*

$$\prod_{v \in S} \min\{1, |\alpha - \beta|_{v'}\}^{d_v} < H(\beta)^{-d(2+\varepsilon)}.$$

Remark 3.0.2. Note that we may replace the right hand side by $CH(\beta)^{-[K:\mathbb{Q}](2+\varepsilon)}$ for any constant $C > 0$. The argument has been given in one of the exercises, but we recall it here again. In the notation from Roth's Theorem 3.0.1, we assume that $\beta \in K$ satisfies

$$\prod_{v \in S} \min\{1, |\alpha - \beta|_{v'}\}^{d_v} < CH(\beta)^{-[K:\mathbb{Q}](2+\varepsilon)} = \frac{C}{H(\beta)^{[K:\mathbb{Q}]\varepsilon/2}} H(\beta)^{-[K:\mathbb{Q}](2+\frac{\varepsilon}{2})}. \tag{3.1}$$

Then β satisfies

$$H(\beta) \leq C^{2/(\varepsilon[K:\mathbb{Q}])} \quad \text{or} \quad \prod_{v \in S} \min\{1, |\alpha - \beta|_{v}\}^{d_v} < H(\beta)^{-[K:\mathbb{Q}](2+\frac{\varepsilon}{2})}.$$

By Northcott's Theorem 2.3.8 there are at most finitely many $\beta \in K$ satisfying the first condition, and by Roth's Theorem 3.0.1 for $\varepsilon/2$ there are at most finitely many $\beta \in K$ satisfying the second condition. This proves that there are indeed at most finitely many $\beta \in K$ satisfying (3.1).

Remark 3.0.3. Let v be an absolute value on the number field K, and $\alpha \in \overline{\mathbb{Q}}$ such that $\alpha \notin K_v$. This means that α is not in the completion of K with respect to v. In particular, there is a positive constant $c > 0$ such that $|\alpha - \beta|_v > c$ for all $\beta \in K_v$. Concerning Roth's theorem, this tells us two things:

- Whenever $\alpha \notin K_v$ for some $v \in S$, then this v does not provide any good approximations. Hence, we can always assume that $\alpha \in K_v$ for all $v \in S$.
- This fact is taken care about in our formulation of Roth's theorem, by taking d_v as an exponent on the left hand side instead of $d_{v'}$: If $\alpha \in K_v$, then both local degrees d_v and $d_{v'}$ are the same for some choice of v'.

We already have seen how we can use this theorem in order to prove the transcendence of certain complex numbers. In this chapter we will finally prove Roth's theorem 3.0.1. Before we give the proof, we will study a further application.

3.1 Thue equations

The classical Thue equation is given by $F(x,y) = m$, where $F(x,y) \in \mathbb{Z}[x,y]$ is an irreducible homogeneous polynomial of degree $n \geq 3$, and $m \in \mathbb{Z} \setminus \{0\}$. We will apply Roth's Theorem 3.0.1 to prove that such equation has at most finitely many integral solutions. Since, Roth's theorem is valid over number fields, we will actually prove a generalization of this result. We recall a special case of a theorem stated on one of the exercise sheets, namely:

Theorem 3.1.1. *Let $f \in \overline{\mathbb{Q}}[x]$ be a polynomial of degree n. Then there is a constant c_f such that for all $\alpha \in \overline{\mathbb{Q}}$ we have*

$$H(\alpha)^n \cdot c_f^{-1} \leq H(f(\alpha)) \leq H(\alpha)^n \cdot c_f.$$

Proof. We should have proven this earlier, so it is tempting to skip the proof. However, this would feel like cheating, too much. So here it is:
Let $f \in \overline{\mathbb{Q}}[x]$ be of degree n, and let $\alpha \in \overline{\mathbb{Q}}$ be arbitrary. We fix any number field K such that $f \in K[x]$ and $\alpha \in K$. We set $d = [K : \mathbb{Q}]$. If f is constant, then $n = 0$ and the statement is trivial. Hence we may assume that $n \geq 1$.
We will start with proving the upper bound, which follows from the (ultrametric) triangular inequality. Let $v \in M_K$ be archimedean. Then we have

$$\begin{aligned} |f(\alpha)|_v &\leq (n+1) \cdot |f|_v \cdot \max\{1, |\alpha|_v^n\} \\ &\leq (n+1) \cdot \max\{1, |f|_v\} \cdot \max\{1, |\alpha|_v^n\} \\ \implies \quad \max\{1, |f(\alpha)|_v\} &\leq (n+1) \cdot \max\{1, |f|_v\} \cdot \max\{1, |\alpha|_v^n\}. \end{aligned} \tag{3.2}$$

Now, let $v \in M_K$ be non-archimedean. Then we have

$$\begin{aligned} |f(\alpha)|_v &\leq |f|_v \cdot \max\{1, |\alpha|_v^n\} \\ &\leq \max\{1, |f|_v\} \cdot \max\{1, |\alpha|_v^n\} \\ \implies \quad \max\{1, |f(\alpha)|_v\} &\leq \max\{1, |f|_v\} \cdot \max\{1, |\alpha|_v^n\}. \end{aligned} \tag{3.3}$$

Putting these estimates together gives

$$\begin{aligned} H(f(\alpha)) &= \prod_{v \in M_K} \max\{1, |f(\alpha)|_v\}^{d_v/d} \\ &\leq \left(\prod_{\substack{v \in M_K \\ v|\infty}} (n+1)^{d_v/d} \right) \cdot \left(\prod_{v \in M_K} \max\{1, |f|_v\}^{d_v/d} \right) \cdot \left(\prod_{v \in M_K} \max\{1, |\alpha^n|_v\}^{d_v/d} \right) \\ &= (n+1) \cdot H(f) \cdot H(\alpha^n) = (n+1) \cdot H(f) \cdot H(\alpha)^n. \end{aligned}$$

This proves the upper bound with an effective constant $C_1(f) = (n+1)H(f)$.
The main observation for the proof of the lower bound is the following:

Claim: There are polynomials $g_1, g_2 \in K[x]$ of degree at most n such that $x^{2n} = g_1(x)f(x) + g_2(x)$.
We will prove the claim as simple as possible. Writing $f(x) = \sum_{i=0}^{n} a_i x^i$, then we need to construct a polynomial $g_1(x) = \sum_{i=0}^{n} b_i x^i \in K[x]$ such that the degree of $x^{2n} - f(x)g_1(x)$ is at most n. This just means that

$$f(x)g_1(x) = \sum_{i=0}^{2n} \left(\sum_{r+s=i} a_r b_s \right) x^i = x^{2n} + c_n x^n + c_{n-1}x^{n-1} + \ldots + c_0.$$

Hence, we only have to choose $b_0, \ldots, b_n \in K$ such that

$$a_n b_n = \sum_{r+s=2n} a_r b_s = 1 \quad \text{and} \quad \sum_{r+s=k} a_r b_s = 0 \quad \forall\, k \in \{n+1, \ldots, 2n-1\}.$$

But surely there are such elements $b_0, \ldots, b_n$. Since $a_n \neq 0$, we have to take $b_n = a_n^{-1}$. Then we construct $b_{n-1}, b_{n-2}, \ldots, b_0$ inductively, by $b_{n-\ell} = -a_n^{-1} \sum_{i=n-\ell+1}^{n} a_{2n-\ell-i} b_i$. This proves the claim.

Note that the polynomials g_1 and g_2 are given solely in terms of f. Now we prove $H(f(\alpha)) \geq C_2(f)H(\alpha)^n$ for some positive constant $C_2(f)$ not dependent on α. To this end, let $v \in M_K$ be non-archimedean. Then we have

$$\begin{aligned}
|\alpha|_v^{2n} &= |g_1(\alpha)f(\alpha) + g_2(\alpha)|_v \leq \max\{|g_1(\alpha)|_v |f(\alpha)|_v, |g_2(\alpha)|_v\} \\
&\leq \max\{|g_1(\alpha)|_v, |g_2(\alpha)|_v\} \cdot \max\{|f(\alpha)|_v, 1\} \\
&\overset{(3.3)}{\leq} \max\{|g_1|_v, |g_2|_v\} \cdot \max\{1, |\alpha|_v^n\} \cdot \max\{|f(\alpha)|_v, 1\} \\
\implies &\max\{1, |\alpha|_v\}^{2n} \leq \max\{|g_1|_v, |g_2|_v, 1\} \cdot \max\{1, |\alpha|_v\}^n \cdot \max\{|f(\alpha)|_v, 1\} \\
\implies &\max\{1, |\alpha|_v\}^{n} \leq \max\{|g_1|_v, |g_2|_v, 1\} \cdot \max\{|f(\alpha)|_v, 1\}.
\end{aligned}$$

Similarly, if $v \in M_K$ is archimedean, then we have

$$\begin{aligned}
|\alpha|_v^{2n} &= |g_1(\alpha)f(\alpha) + g_2(\alpha)|_v \leq 2\max\{|g_1(\alpha)|_v |f(\alpha)|_v, |g_2(\alpha)|_v\} \\
&\leq 2\max\{|g_1(\alpha)|_v, |g_2(\alpha)|_v\} \cdot \max\{|f(\alpha)|_v, 1\} \\
&\overset{(3.2)}{\leq} 2(n+1)\max\{|g_1|_v, |g_2|_v\} \cdot \max\{1, |\alpha|_v\}^n \cdot \max\{|f(\alpha)|_v, 1\} \\
\implies &\max\{1, |\alpha|_v\}^{2n} \leq 2(n+1)\max\{|g_1|_v, |g_2|_v, 1\} \cdot \max\{1, |\alpha|_v\}^n \cdot \max\{|f(\alpha)|_v, 1\} \\
\implies &\max\{1, |\alpha|_v\}^{n} \leq 2(n+1)\max\{|g_1|_v, |g_2|_v, 1\} \cdot \max\{|f(\alpha)|_v, 1\}.
\end{aligned}$$

Hence, the proposed inequality is true at each single absolute value. All we have to do next, is to combine all these estimates.

$$\begin{aligned}
H(\alpha)^n &= \prod_{v \in M_K} \left(\max\{1, |\alpha|_v\}^n\right)^{d_v/d} \\
&\leq \prod_{\substack{v \in M_K \\ v|\infty}} (2(n+1))^{d_v/d} \cdot \prod_{v \in M_K} \left(\max\{|g_1|_v, |g_2|_v, 1\}\right)^{d_v/d} \cdot \prod_{v \in M_K} \max\{|f(\alpha)|_v, 1\}^{d_v/d} \\
&= 2(n+1) \cdot \underbrace{\prod_{v \in M_K} \left(\max\{|g_1|_v, |g_2|_v, 1\}\right)^{d_v/d}}_{\leq H(g_1)\cdot H(g_2)} \cdot H(f(\alpha))
\end{aligned}$$

Hence the lower bound is proved, with $C_2(f) = (2(n+1)H(g_1)H(g_2))^{-1}$. Taking c_f as the maximum of $C_1(f)$ and $C_2(f)$ proves the theorem. □

Remark 3.1.2. The statement in the claim above may remind you on Hilbert's Nullstellensatz. Indeed, if you want to prove this statement in higher dimensions (as formulated on the exercise sheet), you can do precisely the same using Hilbert's Nullstellensatz in order to prove the claim.

Theorem 3.1.3. *Let K be a number field of degree d and let $F(x,y) \in K[x,y]$ be homogeneous of degree $n > 2d$, without a multiple linear factor over $\mathbb{C}[x,y]$ and such that $F(1,0) \neq 0$. For any $\gamma \in K^*$ there are at most finitely many pairs $(\alpha,\beta) \in \mathcal{O}_K^2$ such that $F(\alpha,\beta) = \gamma$. As usual $\mathcal{O}_K$ denotes the ring of integers in K.*

Proof. We have $F(x,y) = \sum_{i=0}^{n} a_i x^i y^{n-i}$, for some $a_1, \dots, a_n \in K$. Our assumption guarantees that $a_n = F(1,0) \neq 0$. It follows

$$\frac{1}{y^n} F(x,y) = \sum_{i=0}^{n} a_i \left(\frac{x}{y}\right)^i = a_n(\frac{x}{y} - \alpha_1) \cdots (\frac{x}{y} - \alpha_n),$$

for certain $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}$. In particular, the linear factors of $F(x,y)$ are precisely $(x - \alpha_i y)$ for $i \in \{1, \dots, n\}$. Hence, by assumption the elements $\alpha_1, \dots, \alpha_n$ are pairwise distinct.
Let $N \in \mathbb{N}$ be such that $Na_n \in \mathcal{O}_K$. We have

$$\begin{aligned} F(\alpha,\beta) = \gamma \quad &\iff \quad N^n a_n^{n-1} F(\alpha,\beta) = N^n a_n^{n-1} \gamma \\ &\iff \quad \prod_{i=1}^{n} (Na_n\alpha - Na_n\alpha_i\beta) = N^n a_n^{n-1}\gamma. \end{aligned}$$

Hence, whenever $(\alpha,\beta) \in \mathcal{O}_K^2$ is a solution of $F(x,y) = \gamma$, then $(Na_n\alpha, \beta) \in \mathcal{O}_K^2$ is a solution of $\widetilde{F}(x,y) = N^n a_n^{n-1}\gamma$, where

$$\widetilde{F}(x,y) = \prod_{i=1}^{n} (x - Na_n\alpha_i y) \in K[x,y].$$

In particular, if the latter equation has only finitely many integral solutions, then the original equation has at most finitely many integral solutions. Hence we may assume from now on that $a_n = 1$.
After this reduction step, we can outline the idea for the proof: If we have infinitely many integral solutions $(\alpha,\beta) \in \mathcal{O}_K$ of $F(x,y) = \gamma$, then we have infinitely many very good approximations of one of the elements $\alpha_1, \dots, \alpha_n$. These approximations will be given by α/β.
With this in mind, we should note the following. If $\beta = 0$ then there are at most n different α such that $F(\alpha,0) = \gamma$. Hence, we may assume that $\beta \neq 0$. Moreover, if $F(\alpha,\beta) = \gamma$, and $\lambda \in \overline{\mathbb{Q}}$ is arbitrary, then $F(\lambda\alpha, \lambda\beta) = \lambda^n\gamma$. Hence, for any solution (α,β) there are at most $n-1$ other solutions (α',β') such that $\alpha/\beta = \alpha'/\beta'$. This means, that infinitely many solutions (α,β) of $F(x,y) = \gamma$ lead to infinitely many different elements α/β.
Having said all this, we can start with the actual proof. Let $(\alpha,\beta) \in \mathcal{O}_K^2$ be a solution to $F(x,y) = \gamma$, with $\beta \neq 0$. Then we have

$$\frac{\gamma}{\beta^n} = \frac{1}{\beta^n} F(\alpha,\beta) = (\frac{\alpha}{\beta} - \alpha_1) \cdots (\frac{\alpha}{\beta} - \alpha_n). \tag{3.4}$$

Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be such that $|\beta|_\sigma = |\sigma(\beta)|$ is maximal (i.e. $\sigma(\beta)$ is a largest Galois-conjugate of β). Since $\beta \in \mathcal{O}_K$, the product of all conjugates of β is a rational integer. Hence, not all Galois conjugates of β can be located inside the unit circle. In particular we know $|\beta|_\sigma \geq 1$. For any $j, k \in \{1, \ldots, n\}$ with $j \neq k$ we have

$$\left|\frac{\alpha}{\beta} - \alpha_j\right|_\sigma + \left|\frac{\alpha}{\beta} - \alpha_k\right|_\sigma \geq |\alpha_j - \alpha_k|_\sigma \geq \min_{\substack{1 \leq r < s \leq n \\ \tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}} |\alpha_r - \alpha_s|_\tau =: C_1(F) > 0.$$

Here we apply the assumption, that all the α_i's are pairwise distinct. It follows that at most one of the numbers $\left|\frac{\alpha}{\beta} - \alpha_i\right|_\sigma$ is $< C_1(F)/2$. This means that all but one of these absolute values are $\geq C_1(F)/2$. It follows

$$\min_{1 \leq j \leq n} \left|\frac{\alpha}{\beta} - \alpha_j\right|_\sigma \cdot \left(\frac{C_1(F)}{2}\right)^{n-1} \leq \prod_{i=1}^{n} \left|\frac{\alpha}{\beta} - \alpha_i\right|_\sigma \overset{(3.4)}{=} \frac{|\gamma|_\sigma}{|\beta|_\sigma^n},$$

and hence

$$\min_{1 \leq j \leq n} \left|\frac{\alpha}{\beta} - \alpha_j\right|_\sigma \leq \left(\frac{2}{C_1(F)}\right)^{n-1} \cdot \frac{|\gamma|_\sigma}{|\beta|_\sigma^n}. \tag{3.5}$$

Now *assume that there are infinitely many integral solutions* (α, β) of $F(x, y) = \gamma$. Then, by the box principle, there is one $k \in \{1, \ldots, n\}$ such that

$$\min_{1 \leq j \leq n} \left|\frac{\alpha}{\beta} - \alpha_j\right|_\sigma = \left|\frac{\alpha}{\beta} - \alpha_k\right|_\sigma$$

for infinitely many pairs $(\alpha, \beta) \in \mathcal{O}_K^2$. We rename the indices to assume $k = 1$. Taking our remarks at the beginning into account, and applying (3.5) we find that there are infinitely many numbers $\alpha/\beta \in K$, with $\alpha, \beta \in \mathcal{O}_K$, such that

$$\left|\frac{\alpha}{\beta} - \alpha_1\right|_\sigma \leq \frac{C_2(F, \gamma)}{|\beta|_\sigma^n}, \quad \text{with} \tag{3.6}$$

$$C_2(F, \gamma) = \left(\frac{2}{C_1(F)}\right)^{n-1} \cdot \max_{\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} |\gamma|_\tau .$$

That already looks like too many good approximations of α_1. We are left to compare $|\beta|_\sigma$ with $M(\alpha/\beta)$. Here the mysterious choice of σ comes into play:

$$|\beta|_\sigma^n = \underbrace{|\sigma(\beta)|^n}_{= \max\{1, |\sigma(\beta)|\}^n} \geq \prod_{\tau \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(\beta), \mathbb{C})} \max\{1, |\tau(\beta)|\}^{n/[\mathbb{Q}(\beta):\mathbb{Q}]} \overset{\beta \in \mathcal{O}_K}{=} H(\beta)^n.$$

Define the polynomial $f(x) = F(x, 1) = (x - \alpha_1) \cdots (x - \alpha_n)$. Then there exists a positive constant $C_3(F)$ only depending on F, such that

$$H(\gamma) + \underbrace{H(\beta^n)}_{= H(\beta^{-n})} \geq H(\gamma \cdot \beta^{-n}) \overset{(3.4)}{=} H(f(\frac{\alpha}{\beta})) \overset{3.1.1}{\geq} H(\frac{\alpha}{\beta})^n \cdot C_3(F).$$

We conclude

$$|\beta|_\sigma^n \geq H(\frac{\alpha}{\beta})^n C_3(F) - H(\gamma).$$

Together with (3.6), this gives for infinitely many numbers $\alpha/\beta \in K$ the estimate

$$\left|\frac{\alpha}{\beta} - \alpha_1\right|_\sigma \leq \frac{C_2(F,\gamma)}{H(\frac{\alpha}{\beta})^n C_3(F) - H(\gamma)} = \frac{\frac{C_2(F,\gamma)}{C_3(F)}}{H(\frac{\alpha}{\beta})^n - C_3(F)^{-1}H(\gamma)}. \tag{3.7}$$

By Northcott's theorem 2.3.8, there are at most finitely many elements $\alpha/\beta \in K$ such that $\frac{1}{2}H(\alpha/\beta)^n \leq H(\gamma)C_3(F)^{-1}$. Hence, if there are infinitely many $\alpha/\beta \in K$ satisfying (3.7), then there must be infinitely many $\alpha/\beta \in K$ such that

$$\left|\frac{\alpha}{\beta} - \alpha_1\right|_\sigma \leq \frac{\frac{C_2(F,\gamma)}{2C_3(F)}}{H(\frac{\alpha}{\beta})^n} = \frac{\frac{C_2(F,\gamma)}{2C_3(F)}}{H(\frac{\alpha}{\beta})^{d\cdot\frac{n}{d}}}$$

Since $n/d > 2$, by or assumption, this contradicts Roth's Theorem 3.0.1 (cf. Remark 3.0.2). Hence, there are at most finitely many solutions $(\alpha, \beta) \in \mathcal{O}_K^2$ of the equation $F(x, y) = \gamma$. □

Remark 3.1.4. The polynomials handled in Theorem 3.1.3 are indeed a generalization of the original Thue equations. Choose $K = \mathbb{Q}$ in the theorem and let $F(x, y) \in \mathbb{Z}[x, y]$ be irreducible and homogeneous of degree $n \geq 3 > 2[\mathbb{Q} : \mathbb{Q}]$. Since, F is irreducible and $\mathbb{Q}$ is a perfect field, there are no multiple linear factors of F in $\mathbb{C}[x, y]$. Write $F(x, y) = \sum_{i=0}^n a_i x^i y^{n-i}$. If $a_n = F(1, 0) = 0$, then $F(x, y) = \sum_{i=0}^{n-1} a_i x^i y^{n-i} = y \cdot \sum_{i=0}^{n-1} a_i x^i y^{n-i-1}$ contradicting the fact that F is irreducible. Hence, F is indeed handled in Theorem 3.1.3.
However, we do not need the full force of Roth's theorem to prove that a Thue equation has at most finitely many solutions. But still we need more than Liouville's approximation.

Remark 3.1.5. This result can be extended further in several ways. For instance, with almost the same proof one can show, that the equation $F(x, y) = \gamma$ as in Theorem 3.1.3 has only finitely many solutions in the S-integers $\mathcal{O}_{K,S}$ for any finite set $S \subseteq M_K^{\text{fin}}$.

As an example I could write down any Thue equation like $x^3 - 3yx^2 + 5y^2x - 2y^3 = 1$, and now we know that there are at most finitely many integral solutions to this equation. But most likely, you would not be very enthusiastic about this result. So let me give you another, non-obvious, application of this result. We study the question, how often the sum of two algebraic units is again an algebraic unit. Let us try to make this more precise, by studying a simple example.

Example 3.1.6. Let $n \in \mathbb{N}$ be odd and denote with ζ_n a primitive nth root of unity. By Euler's theorem we have $2^{\varphi(n)} \equiv 1 \mod n$, where φ is Eulers-Phi-Function. Hence $\zeta_n = \zeta_n^{2^{\varphi(n)}}$. We compute

$$\underbrace{\left(\frac{\zeta_n^2 - 1}{\zeta_n - 1}\right)}_{=\zeta_n+1} \cdot \underbrace{\left(\frac{\zeta_n^4 - 1}{\zeta_n^2 - 1}\right)}_{=\zeta_n^2+1} \cdot \ldots \cdot \underbrace{\left(\frac{\zeta_n^{2^{\varphi(n)}} - 1}{\zeta_n^{2^{\varphi(n)-1}} - 1}\right)}_{=\zeta_n^{2^{\varphi(n)-1}}+1} = \left(\frac{\zeta_n^{2^{\varphi(n)}} - 1}{\zeta_n - 1}\right) = 1.$$

In particular, $\zeta_n + 1$ is always an algebraic unit (and so are ζ_n and 1).

This example shows that there are infinitely many pairs of algebraic units, such that the sum is again an algebraic unit. However, the examples we have found do not lie in a fixed number field. So maybe we should ask: For a given number field K, are there still infinitely many $\alpha, \beta \in \mathcal{O}_K^*$ such that $\alpha + \beta \in \mathcal{O}_K^*$ as well? This was answered in the negative by Siegel. By multiplying with the inverse of $\alpha + \beta$, one may equivalently ask for solutions $\alpha, \beta \in \mathcal{O}_K^*$ of the equation $x + y = 1$. This is the so-called *unit-equation*.

Theorem 3.1.7. *Let K be a number field. There are at most finitely many $\alpha, \beta \in \mathcal{O}_K^*$ such that $\alpha + \beta = 1$.*

Proof. We have to solve the equation $x + y = 1$. The left hand side is indeed a homogeneous polynomial in two variables, but the degree is equal to 1, and not ≥ 3. So at fist sight, Thue-equations do not seem to be an appropriate tool. We will artificially introduce an appropriate exponent n to this equation.
Let us start with applying the first thing that comes to mind, when we see $\mathcal{O}_K^*$: Dirichlet's unit theorem. This is, $\mathcal{O}_K^*$ is finitely generated, and has rank $r+s-1$, where r is the number of real embeddings of K and s is the number of complex embeddings of K. Alternatively, we can describe $r + s$ as the number of archimedean absolute values in M_K.
Since $\mathcal{O}_K^*$ is finitely generated, the quotient group $\mathcal{O}_K^*/(\mathcal{O}_K^*)^n$ is finite for all $n \in \mathbb{N}$, where $(\mathcal{O}_K^*)^n = \{\epsilon^n | \epsilon \in \mathcal{O}_K^*\}$ denotes the subgroup of nth powers in $\mathcal{O}_K^*$.
For all $n \in \mathbb{N}$, we denote with $\mathcal{R}_n \subseteq \mathcal{O}_K^*$ a full set of representatives of the elements in the quotient $\mathcal{O}_K^*/(\mathcal{O}_K^*)^n$. Hence, if $\alpha \in \mathcal{O}_K^*$, then there is an unique $a \in \mathcal{R}_n$ and an $\epsilon \in \mathcal{O}_K^*$ such that $\alpha = a\epsilon^n$.
So finally we have introduced our nth power. Hence, having the Thue-equation in mind, we fix some integer $n > 2[K : \mathbb{Q}]$. We see that

$$\begin{aligned} & \alpha + \beta = 1 \quad \text{for } \alpha, \beta \in \mathcal{O}_K^* \\ \iff \quad & a\epsilon^n + b\delta^n = 1 \quad \text{for some } a, b \in \mathcal{R}_n \text{ and } \epsilon, \delta \in \mathcal{O}_K^*. \end{aligned}$$

Recall that $\mathcal{R}_n$ is finite. Hence, any solution $\alpha, \beta \in \mathcal{O}_K^*$ of $x + y = 1$, gives rise to a solution $\epsilon, \delta \in \mathcal{O}_K^*$ of one of the finitely many equations

$$ax^n + by^n = 1 \quad \text{with } a, b \in \mathcal{R}_n. \tag{3.8}$$

Since any of these equations factors as $ax^n + by^n = a\prod_{i=1}^n (x - \zeta_n^i \sqrt[n]{-b/a}\, y)$ for some choice of the nth root of $-b/a$, all linear factors of any of these equations are pairwise distinct. Now we can apply Theorem 3.1.3, and conclude that the finitely many equations from (3.8) have only finitely many solutions in $\mathcal{O}_K$ (and in particular in $\mathcal{O}_K^*$). Hence, there are at most finitely many solutions of $x + y = 1$ in the algebraic units $\mathcal{O}_K^*$. □

Remark 3.1.8. As before we state that with minor changes in the proof, we see that there are at most finitely many S-units in K that sum up to another S-unit, for any finite set $S \subseteq M_K^{\text{fin}}$.

We close this section with an outline of the proof of Roth's theorem:

(1) Assume there are many good approximations of a given $\alpha \in \overline{\mathbb{Q}}$ – say m. Then we construct a polynomial $P \in \mathbb{Z}[x_1, \ldots, x_m]$ that vanishes at $\underline{\alpha} = (\alpha, \ldots, \alpha) \in \overline{\mathbb{Q}}^m$ to a very large order (more precisely: with a very large index).

(2) If $\beta_1, \ldots, \beta_m \in K$ are the good approximations of α, we aim to prove that P does not vanish at $\underline{\beta} = (\beta_1, \ldots, \beta_m)$.

(3) Then $P(\underline{\beta})$ is not too small in terms of the β_i's (gap principle). Note that we can assume that the height of all the β_i's is very large, since there are only finitely many elements in K of bounded height.

(4) But since P vanishes at $\underline{\alpha}$ with a large index, the Taylor expansion of P at $\underline{\alpha}$ can be used to prove that $P(\underline{\beta})$ is very close to zero (with large enough m). If it is too close to zero, we hopefully get something which contradicts (3).

Of course, the polynomial P should be constructed using Siegel's Lemma 2.4.6 (cf. Theorem 2.6.5). However, in sharp contrast to the case of polynomials in one variable, there is no reason why $P(\underline{\beta})$ should not be zero. One of the ingenious ideas in the proof is the observation, that it might be zero, but the index at $\underline{\beta}$ should be considerable smaller than the index from (1). Then the argument outlined above applies for some derivative of P! To prove that the index of P at β is small (a result known as Roth's lemma), is the hardest part of the proof.

Exercises

Exercise 3.1. (a) Prove that there are at most finitely many solutions $(\alpha, \beta) \in \mathbb{Z}^2$ of the equation

$$x^5 + 4x^4y + y - 6x^3y^2 - y^2 + 8xy^4 - 2y^5 - 1 = 0.$$

(b) Formulate a general statement about finiteness of integral solutions of a class of Diophantine equations, which contains the above equation.

(c) Are there finitely many or infinitely many integral solutions of the equation

$$x^4 - 4x^2y^2 + 4y^4 = 16?$$

3.2 Preliminaries I – Multivariable Polynomial Estimates

We already know quite a bit about heights. But so far, we have not really worked with the height of multivariable polynomials. Above we claimed that a polynomial $P \in \overline{\mathbb{Q}}[x_1, \dots, x_n]$ with certain vanishing properties and of small height, will play an essential role in the proof of Roth's theorem. The vanishing properties of a polynomial do not change if we multiply the polynomial with some non-negative constant. Hence, once we have found a polynomial with good vanishing properties, we should multiply it with an appropriate constant, to reduce its height. Alternatively, we could consider the set of polynomials $\lambda \cdot P$ as an equivalence class of the polynomial P, and define a height for this equivalence class.

Definition 3.2.1. For $f \in \overline{\mathbb{Q}}[x_1, \dots, x_n] \setminus \{0\}$ we define the *multiplicative projective height* of f to be the quantity

$$H_{\mathbb{P}}(f) = \prod_{v \in M_K} |f|_v^{d_v/[K:\mathbb{Q}]},$$

for any number field K that contains all coefficients of f. The *logarithmic projective height* of f is, as usual $h_{\mathbb{P}}(f) = \log(H_{\mathbb{P}}(f))$.

The projective height of a polynomial is calculated by considering its coefficients as coordinates of a point in a projective space, and then calculate the height of this point.

Lemma 3.2.2. *For any $f \in \overline{\mathbb{Q}}[x_1, \dots, x_n] \setminus \{0\}$ we have*

$$H_{\mathbb{P}}(f) = \min_{\lambda \in \overline{\mathbb{Q}}^*} H(\lambda \cdot f).$$

Proof. This is given as an exercise. □

Given polynomials $f_1, \dots, f_r \in \overline{\mathbb{Q}}[x_1, \dots, x_n]$, we want to compare the (projective) heights of the f_i's with the height of $f = f_1 \cdots f_r$. The non-archimedean part of the heights can be easily compared by the Gauß-Lemma 2.3.2, since for any non-archimedean $v \in M_K$ we have $|f|_v = |f_1|_v \cdots |f_r|_v$, where K is any number field with $f_1, \dots, f_r \in K[x_1, \dots, x_n]$. What is still missing, is an archimedean version of the Gauß-Lemma.
We know from Proposition 2.1.17, that we can express the Mahler measure of some α analytically in terms of it's minimal polynomial f, by $M(\alpha) = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log\left|f(e^{i\theta})\right| \mathrm{d}\theta\right)$. The right-hand-side of course only depends on the polynomial f. So in particular, we can define the Mahler measure of any polynomial $f \in \mathbb{C}[x]$ by this formula. This is:

$$M(f) = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log\left|f(e^{i\theta})\right| \mathrm{d}\theta\right) \quad \forall\ f \in \mathbb{C}[x].$$

We want to study multivariable polynomials. Luckily, the definition above readily generalizes to the case of multivariable polynomials.

Definition 3.2.3. For all $f \in \mathbb{C}[x_1, \dots, x_n]$ we define the *Mahler measure* of f to be the quantity

$$M(f) = \exp\left(\frac{1}{(2\pi)^n}\int_0^{2\pi} \cdots \int_0^{2\pi} \log\left|f(e^{i\theta_1}, \dots, e^{i\theta_n})\right| \mathrm{d}\theta_1 \cdots \mathrm{d}\theta_n\right).$$

Keeping in mind that we want to compare the heights of $f_1 \cdots f_r$ with the heights of the factors $f_1, \dots, f_r$, the Mahler measure seems to be a promising tool. We know that it is somehow linked to the height, and obviously, we have

$$M(f_1 \cdots f_r) = M(f_1) \cdots M(f_r). \tag{3.9}$$

We will use two results from complex analysis as a black box.

Theorem 3.2.4. *Let $f \in \mathbb{C}[x_1, \dots, x_n]$. As usual we write $f = \sum_{\underline{k} \in \mathbb{N}_0^n} a_{\underline{k}} \underline{x}^{\underline{k}}$, with $\underline{x}^{\underline{k}} = x_1^{k_1} \cdots x_n^{k_n}$ for $\underline{k} = (k_1, \dots, k_n)$. Then we have*

(a) (Parseval's formula)

$$\left(\frac{1}{2\pi}\right)^n \int_0^{2\pi} \cdots \int_0^{2\pi} \left|f(e^{i\theta_1}, \dots, e^{i\theta_n})\right|^2 \mathrm{d}\theta_1 \cdots \mathrm{d}\theta_n = \sum_{\underline{k} \in \mathbb{N}_0^n} |a_{\underline{k}}|^2.$$

(b) (Jensen's inequality)

$$M(f)^2 \leq \left(\frac{1}{2\pi}\right)^n \int_0^{2\pi} \cdots \int_0^{2\pi} \left|f(e^{i\theta_1}, \dots, e^{i\theta_n})\right|^2 \mathrm{d}\theta_1 \cdots \mathrm{d}\theta_n.$$

Remark 3.2.5. Both statements are special cases of general analytic results (non of which is particularly difficult to prove). For instance, Jensen's inequality states that for any convex function $\varphi : \mathbb{R} \to \mathbb{R}$, and any probability space (Ω, μ) we have $\varphi\left(\int_\Omega g \mathrm{d}\mu\right) \leq \int_\Omega \varphi \circ g \mathrm{d}\mu$ for all μ-integrable functions $g : \Omega \to \mathbb{R}$. Hence statement (b) follows from noticing, that exp(.) is convex.

Corollary 3.2.6. *For any $f \in \mathbb{C}[x_1, \ldots, x_n]$ we have*

$$M(f) \leq \left(\prod_{i=1}^{n} (\deg_{x_i}(f) + 1) \right)^{1/2} \cdot |f| \,.$$

Proof. We again write $f = \sum_{\underline{k} \in \mathbb{N}_0^n} a_{\underline{k}} \underline{x}^{\underline{k}}$. Combining part (a) and part (b) from Theorem 3.2.4, we get

$$M(f) \leq \left(\sum_{\underline{k} \in \mathbb{N}_0^n} |a_{\underline{k}}|^2 \right)^{1/2}. \tag{3.10}$$

At most $\prod_{i=1}^{n} (\deg_{x_i}(f) + 1)$ of the coefficients of f are non-zero, and by definition of $|f|$ all coefficients of f are of absolute value $\leq |f|$. Using this in formula (3.10) gives the claimed bound

$$M(f) \leq \left(\prod_{i=1}^{n} (\deg_{x_i}(f) + 1) \right)^{1/2} \cdot |f| \,.$$

□

We know from Lemma 2.1.7 that the i's coefficient a_i of a one-variable polynomial f of degree d satisfies $|a_i| \leq \binom{d}{i} M(f) \leq \binom{d}{\lfloor d/2 \rfloor} M(f)$. We generalize this to polynomials in n variables.

Lemma 3.2.7. *Let $f \in \mathbb{C}[x_1, \ldots, x_n]$, with $\deg_{x_i}(f) \leq r_i$ for all $i \in \{1, \ldots, n\}$, for certain integers $r_1, \ldots, r_n$. Then*

$$|f| \leq \prod_{i=1}^{n} \binom{r_n}{\lfloor r_n/2 \rfloor} \cdot M(f).$$

Proof. We prove this by induction on the number of variables n. As mentioned before, the induction base has already be done in Lemma 2.1.7. Hence, we assume that the statement is true for all polynomials in less than n variables.
There are polynomials $f_0, \ldots, f_{r_n} \in \mathbb{C}[x_1, \ldots, x_{n-1}]$ such that

$$f = \sum_{k=0}^{r_n} f_k(x_1, \ldots, x_{n-1}) \cdot x_n^k.$$

We first note that the set of coefficients of f is precisely the set of coefficients of all the f_k's. This just means

$$|f| = \max_{0 \leq k \leq r_n} |f_k| \,. \tag{3.11}$$

For any choice of real numbers $\theta_1, \ldots, \theta_{n-1}$, we apply our induction base to get

$$M(f(e^{i\theta_1}, \ldots, e^{i\theta_{n-1}}, x_n)) \geq \max_{0 \leq k \leq r_n} \left| f_k(e^{i\theta_1}, \ldots, e^{i\theta_{n-1}}) \right| \cdot \binom{r_n}{\lfloor r_n/2 \rfloor}^{-1}. \tag{3.12}$$

We split the multiple integrals in the definition of the Mahler measure of f to get

$$\begin{aligned}
&\log(M(f))\\
&\overset{\text{Def}}{=} \frac{1}{(2\pi)^{n-1}} \underbrace{\int_0^{2\pi} \cdots \int_0^{2\pi}}_{(n-1)\text{-times}} \frac{1}{2\pi} \int_0^{2\pi} \log\left|f(e^{i\theta_1},\ldots,e^{i\theta_n})\right| \mathrm{d}\theta_n \mathrm{d}\theta_1 \cdots \mathrm{d}\theta_{n-1}\\
&\overset{\text{Def}}{=} \frac{1}{(2\pi)^{n-1}} \int_0^{2\pi} \cdots \int_0^{2\pi} \log(M(f(e^{i\theta_1},\ldots,e^{i\theta_{n-1}},x_n)))\mathrm{d}\theta_1 \cdots \mathrm{d}\theta_{n-1}\\
&\overset{(3.12)}{\geq} \frac{1}{(2\pi)^{n-1}} \int_0^{2\pi} \cdots \int_0^{2\pi} \log\left(\max_{0\leq k\leq r_n}\left|f_k(e^{i\theta_1},\ldots,e^{i\theta_{n-1}})\right| \cdot \binom{r_n}{\lfloor r_n/2\rfloor}^{-1}\right) \mathrm{d}\theta_1 \cdots \mathrm{d}\theta_{n-1}\\
&= \frac{1}{(2\pi)^{n-1}} \int_0^{2\pi} \cdots \int_0^{2\pi} \max_{0\leq k\leq r_n} \log\left(\left|f_k(e^{i\theta_1},\ldots,e^{i\theta_{n-1}})\right|\right) \mathrm{d}\theta_1 \cdots \mathrm{d}\theta_{n-1} + \log(\binom{r_n}{\lfloor r_n/2\rfloor}^{-1})\\
&\geq \max_{0\leq k\leq r_n} \frac{1}{(2\pi)^{n-1}} \int_0^{2\pi} \cdots \int_0^{2\pi} \log\left(\left|f_k(e^{i\theta_1},\ldots,e^{i\theta_{n-1}})\right|\right) \mathrm{d}\theta_1 \cdots \mathrm{d}\theta_{n-1} + \log(\binom{r_n}{\lfloor r_n/2\rfloor}^{-1})\\
&= \max_{0\leq k\leq r_n} \log(M(f_k)) + \log(\binom{r_n}{\lfloor r_n/2\rfloor}^{-1}).
\end{aligned}$$

This implies

$$\begin{aligned}
M(f) &\geq \max_{0\leq k\leq r_n} M(f_k) \cdot \binom{r_n}{\lfloor r_n/2\rfloor}^{-1} \overset{\text{IH}}{\geq} \max_{0\leq k\leq r_n} |f_k| \cdot \left(\prod_{i=1}^{n-1} \binom{r_i}{\lfloor r_i/2\rfloor}^{-1}\right) \cdot \binom{r_n}{\lfloor r_n/2\rfloor}^{-1}\\
&\overset{(3.11)}{=} |f| \cdot \left(\prod_{i=1}^{n} \binom{r_i}{\lfloor r_i/2\rfloor}\right)^{-1},
\end{aligned}$$

and hence the claim. □

Lemma 3.2.8. *Let $r_1,\ldots,r_n \in \mathbb{N}_0$ be arbitrary. Then we have*

$$\binom{r_1}{\lfloor r_1/2\rfloor} \cdots \binom{r_n}{\lfloor r_n/2\rfloor} \leq \binom{r_1+\ldots+r_n}{\lfloor (r_1+\ldots+r_n)/2\rfloor}.$$

Proof. We only have to prove the case $n = 2$, then the result follows immediately by induction. Consider the polynomial equation

$$(1+x)^{r_1} \cdot (1+x)^{r_2} = (1+x)^{r_1+r_2}.$$

The $a = \lfloor r_1/2\rfloor + \lfloor r_2/2\rfloor$ coefficient of the left hand side is $\sum_{k+\ell=a} \binom{r_1}{k}\binom{r_2}{\ell} \geq \binom{r_1}{\lfloor r_1/2\rfloor}\binom{r_2}{\lfloor r_2/2\rfloor}$. But the left hand side tells us that every coefficient of this polynomial is less or equal to $\binom{r_1+r_2}{\lfloor (r_1+r_2)/2\rfloor}$. This proves the lemma. □

Lemma 3.2.9. *For any $d \in \mathbb{N}_0$ we have $\binom{d}{\lfloor d/2\rfloor}\sqrt{d+1} \leq 2^d$.*

Proof. The estimate is obviously true for $d = 0$ and $d = 1$. Now the statement is true for all even $d = 2d'$, which can be proved by induction on d'. Then one shows that this implies the statement for all odd d as well. The details are left as an exercise. □

Lemma 3.2.10. *Let $f_1, \dots, f_r \in \mathbb{C}[x_1, \dots, x_n]$ be arbitrary, and define $f = f_1 \cdots f_r$. Then we have*

$$|f_1| \cdots |f_r| \leq 2^{\deg_{x_1}(f)+\dots+\deg_{x_n}(f)} |f| .$$

Proof. We have to combine all the estimates we have established in this section. To this end, set $r_i(j) := \deg_{x_i}(f_j)$ for all $(i,j) \in \{1, \dots, n\} \times \{1, \dots, r\}$. Then

$$\sum_{j=1}^{r} r_i(j) = \deg_{x_i}(f) \quad \forall\, i \in \{1, \dots, n\}. \tag{3.13}$$

Now we can start:

$$\begin{aligned}
\prod_{j=1}^{r} |f_j| &\overset{3.2.7}{\leq} \prod_{j=1}^{r} \prod_{i=1}^{n} \binom{r_i(j)}{\lfloor r_i(j)/2 \rfloor} M(f_j) = \left(\prod_{j=1}^{r} \prod_{i=1}^{n} \binom{r_i(j)}{\lfloor r_i(j)/2 \rfloor} \right) \cdot \prod_{j=1}^{r} M(f_j) \\
&\overset{(3.9)}{=} \left(\prod_{j=1}^{r} \prod_{i=1}^{n} \binom{r_i(j)}{\lfloor r_i(j)/2 \rfloor} \right) \cdot M(f) \\
&\overset{3.2.6}{\leq} \left(\prod_{i=1}^{n} \prod_{j=1}^{r} \binom{r_i(j)}{\lfloor r_i(j)/2 \rfloor} \right) \cdot \left(\prod_{i=1}^{n} (\deg_{x_i}(f) + 1) \right)^{1/2} \cdot |f| \\
&\overset{3.2.8,(3.13)}{\leq} \left(\prod_{i=1}^{n} \binom{\deg_{x_i}(f)}{\lfloor \deg_{x_i}(f)/2 \rfloor} \right) \cdot \left(\prod_{i=1}^{n} \sqrt{\deg_{x_i}(f) + 1} \right) \cdot |f| \\
&= \prod_{i=1}^{n} \left(\binom{\deg_{x_i}(f)}{\lfloor \deg_{x_i}(f)/2 \rfloor} \cdot \sqrt{\deg_{x_i}(f) + 1} \right) \cdot |f| \\
&\overset{3.2.9}{\leq} \left(\prod_{i=1}^{n} 2^{\deg_{x_i}(f)} \right) \cdot |f| .
\end{aligned}$$

This is what we wanted to prove. □

Remark 3.2.11. A straight forward computation, which we avoid in this lecture, also gives the estimate

$$|f_1| \cdots |f_r| \geq 2^{-(\deg_{x_1}(f)+\dots+\deg_{x_n}(f))} |f| ,$$

with the notation from Lemma 3.2.10.

Finally, we can prove the main result in this section.

Proposition 3.2.12 (Gelfond's Lemma)**.** *Let $f_1, \dots, f_r \in \overline{\mathbb{Q}}[x_1, \dots, x_n]$, and define $f = f_1 \cdots f_r$. Then we have*

$$H_{\mathbb{P}}(f) \geq 2^{-(\deg_{x_1}(f)+\dots+\deg_{x_n}(f))} \prod_{j=1}^{r} H_{\mathbb{P}}(f_j).$$

Proof. This (at least) follows immediately from the Gauß Lemma 2.3.2 and Lemma 3.2.10. We fix any number field K such that $f_1, \dots, f_r \in K[x_1, \dots, x_n]$. The degree of K is denoted by d. Note that for any archimedean $v \in M_K$ we can use the estimate from Lemma 3.2.10, since for any polynomial $g \in K[x_1, \dots, x_n]$ we have $|g|_v = |\sigma(g)|$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$.

Now we conclude

$$\begin{aligned}\prod_{j=1}^{r} H_{\mathbb{P}}(f_j) &= \prod_{v\in M_K} \left(|f_1|_v \cdots |f_r|_v\right)^{d_v/d} = \prod_{\substack{v\in M_K\\ v|\infty}} \left(|f_1|_v \cdots |f_r|_v\right)^{d_v/d} \cdot \prod_{\substack{v\in M_K\\ v\nmid\infty}} \left(|f_1|_v \cdots |f_r|_v\right)^{d_v/d} \\ &\overset{2.3.2}{=} \prod_{\substack{v\in M_K\\ v|\infty}} \left(|f_1|_v \cdots |f_r|_v\right)^{d_v/d} \cdot \prod_{\substack{v\in M_K\\ v\nmid\infty}} |f|_v^{d_v/d} \\ &\overset{3.2.10}{\leq} \prod_{\substack{v\in M_K\\ v|\infty}} \left(2^{\deg_{x_1}(f)+\ldots+\deg_{x_n}(f)}\right)^{d_v/d} \cdot \prod_{v\in M_K} |f|_v^{d_v/d} \\ &= 2^{\deg_{x_1}(f)+\ldots+\deg_{x_n}(f)} \cdot H_{\mathbb{P}}(f).\end{aligned}$$

This proves the proposition. □

Remark 3.2.13. If we apply Remark 3.2.11 instead of Lemma 3.2.10, then, in the notation from Proposition 3.2.12, we get

$$H_{\mathbb{P}}(f) \leq 2^{\deg_{x_1}(f)+\ldots+\deg_{x_n}(f)} \prod_{j=1}^{r} H_{\mathbb{P}}(f_j).$$

Exercises

Exercise 3.2. Prove that for all $f \in \overline{\mathbb{Q}}[x_1, \ldots, x_n] \setminus \{0\}$, we have

$$H_{\mathbb{P}}(f) = \min_{\lambda\in\overline{\mathbb{Q}}^*} H(\lambda \cdot f).$$

Exercise 3.3. Let $n > k \geq 1$ be integers, and let $\overline{\mathbb{Q}}[x_1, \ldots, x_n]$ be the polynomial ring in n variables. Prove that for all $f \in \overline{\mathbb{Q}}[x_1, \ldots, x_k]$ and all $g \in \overline{\mathbb{Q}}[x_{k+1}, \ldots, x_n]$, we have $H_{\mathbb{P}}(f) \cdot H_{\mathbb{P}}(g) = H_{\mathbb{P}}(f \cdot g)$.

Exercise 3.4. Prove Lemma 3.2.9.

3.3 Preliminaries II – Linearly Independent Polynomials

We know that for any field F the polynomial ring $F[x_1, \ldots, x_n]$ is an F-vector space. We want to find a tool which will help us to decide whether a set of polynomials in $F[x_1, \ldots, x_n]$ is F-linearly independent or not. The main result in this section has its origin in the theory of ordinary partial differential equations. We will only sketch the proofs.
In this section we always assume that F is a subfield of $\mathbb{C}$. Let us first study the case of a single variable.

Definition 3.3.1. Let $f_1, \ldots, f_m \in F[x]$, then the *Wronskian determinant* of $f_1, \ldots, f_m$ is

$$W(f_1, \ldots, f_m) = \det \begin{pmatrix} f_1^{(0)}(x) & \cdots & f_m^{(0)}(x) \\ \vdots & \ddots & \vdots \\ f_1^{(m-1)}(x) & \cdots & f_m^{(m-1)}(x) \end{pmatrix} \in F[x],$$

where as before $f^{(k)}(x)$ is the kth derivative of f.

Lemma 3.3.2. *If $f_1, \ldots, f_m \in F[x]$ are F-linearly dependent, then $W(f_1, \ldots, f_m) = 0$.*

Proof. This follows from the fact that derivation is a linear operator. Let $c_1, \ldots, c_m \in F$ not all zero satisfy

$$c_1 f_1(x) + \ldots + c_m f_m(x) = 0.$$

Without loss of generality, we may assume $c_m \neq 0$. Then

$$f_m = -\frac{1}{c_m} \sum_{i=1}^{m-1} c_i f_i(x), \quad \text{and hence} \quad f_m^{(k)} = -\frac{1}{c_m} \sum_{i=1}^{m-1} c_i f_i^{(k)}(x) \quad \forall\ k \in \mathbb{N}_0.$$

This means that the last column in the matrix defining $W(f_1, \ldots, f_m)$ is a linear combination of all the other columns. Hence $W(f_1, \ldots, f_m) = 0$. □

The interesting thing is, that also the converse of the preceding lemma is true.

Proposition 3.3.3. *The polynomials $f_1, \ldots, f_m \in F[x]$ are F-linearly independent if and only if $W(f_1, \ldots, f_m) \neq 0$.*

Proof. It is left to prove that $f_1, \ldots, f_m$ are F-linearly dependent, whenever $W(f_1, \ldots, f_m) = 0$. This can be proved by induction on m. The induction base is trivial, since $W(f_1) = f_1 = 0$ if and only if f_1 is linearly dependent. Hence, we may assume that the statement is true for a fixed $m \geq 1$.
Now, assume that $W(f_1, \ldots, f_m, f_{m+1}) = 0$. Combining this with Lemma 3.3.2, we know that $W(f_1, \ldots, f_m, f_i) = 0$ for all $i \in \{1, \ldots, m+1\}$. Expanding the determinants along the last column gives us that for all $i \in \{1, \ldots, m+1\}$ we have

$$0 = f_i^{(0)} \underbrace{\det \begin{pmatrix} f_1^{(1)} & \cdots & f_m^{(1)} \\ \vdots & \ddots & \vdots \\ f_1^{(m)} & \cdots & f_m^{(m)} \end{pmatrix}}_{=V_0(x)} - f_i^{(1)} \underbrace{\det \begin{pmatrix} f_1^{(0)} & \cdots & f_m^{(0)} \\ f_1^{(2)} & \cdots & f_m^{(2)} \\ \vdots & \ddots & \vdots \\ f_1^{(m)} & \cdots & f_m^{(m)} \end{pmatrix}}_{=V_1(x)} + \ldots$$

$$\pm f_i^{(m)} \underbrace{\det \begin{pmatrix} f_1^{(0)} & \cdots & f_m^{(0)} \\ \vdots & \ddots & \vdots \\ f_1^{(m-1)} & \cdots & f_m^{(m-1)} \end{pmatrix}}_{=V_m(x)}.$$

By induction, we may assume that $V_m(x) \neq 0$, since otherwise $f_1, \ldots, f_m$ are F-linearly dependent, and then $f_1, \ldots, f_{m+1}$ are as well. This means that the $f_1, \ldots, f_{m+1}$ are solutions of one homogeneous partial differential equation (PDE) of order m. But the dimension of the F-vector space of solutions of such a PDE has dimension m. Hence, the polynomials $f_1, \ldots, f_{m+1}$ must be F-linearly dependent. □

Recall that for any $f \in F[x_1, \ldots, x_n]$ and any $\underline{d} = (d_1, \ldots, d_n) \in \mathbb{N}_0^n$, we set

$$\partial_{\underline{d}} f = \frac{1}{d_1! \cdots d_n!} \cdot \frac{\partial^{\underline{d}}}{\partial \underline{x}^{\underline{d}}} f \in F[x_1, \ldots, x_n].$$

Definition 3.3.4. For any $\underline{d} = (d_1, \ldots, d_n) \in \mathbb{N}_0^n$, the *order of the operator* $\partial_{\underline{d}}$, is given by $\operatorname{ord}(\partial_{\underline{d}}) = d_1 + \ldots + d_n$.

Definition 3.3.5. Let $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$. Then a *generalized Wronskian determinant of* $f_1, \ldots, f_m$ is given by

$$W_{\underline{d(1)},\ldots,\underline{d(m)}}(f_1, \ldots, f_m) = \det \begin{pmatrix} \partial_{\underline{d(1)}} f_1 & \cdots & \partial_{\underline{d(1)}} f_m \\ \vdots & \ddots & \vdots \\ \partial_{\underline{d(m)}} f_1 & \cdots & \partial_{\underline{d(m)}} f_m \end{pmatrix} \in F[x_1, \ldots, x_n],$$

where for all $i \in \{1, \ldots, m\}$ we have $\operatorname{ord}(\partial_{\underline{d(i)}}) \leq i - 1$.

Remark 3.3.6. Let us consider the case $n = 1$. Then for each i there is precisely one operator $\partial_{\underline{d}} = \partial_i$ of order i. Of course, the generalized Wronskian determinant is zero if $\underline{d(i)} = \underline{d(j)}$ for some $i \neq j$. Hence, a generalized Wronskian determinant of $g_1, \ldots, g_m \in F[x]$ is zero or equal to

$$\begin{aligned} W_{0,1,\ldots,m-1}(g_1, \ldots, g_m) &= \det \begin{pmatrix} \partial_0 g_1 & \cdots & \partial_0 g_m \\ \vdots & \ddots & \vdots \\ \partial_{m-1} g_1 & \cdots & \partial_{m-1} g_m \end{pmatrix} \\ &= \det \begin{pmatrix} \frac{1}{0!} g_1^{(0)} & \cdots & \frac{1}{0!} g_m^{(0)} \\ \vdots & \ddots & \vdots \\ \frac{1}{(m-1)!} g_1^{(m-1)} & \cdots & \frac{1}{(m-1)!} g_m^{(m-1)} \end{pmatrix} \\ &= \left(\prod_{i=0}^{m-1} \frac{1}{i!} \right) \cdot W(g_1, \ldots, g_m). \end{aligned}$$

Theorem 3.3.7. *The polynomials $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$ are F-linearly independent if and only if there is some generalized Wronskian determinant $W_{\underline{d(1)},\ldots,\underline{d(m)}}(f_1, \ldots, f_m)$ not identically zero.*

Proof. That all generalized Wronskian determinants of $f_1, \ldots, f_m$ vanish if the polynomials $f_1, \ldots, f_m$ are F-linearly dependent follows precisely as in Lemma 3.3.2. The other implication can be reduced to the case $n = 1$, as follows.
Let $d \in \mathbb{N}$ be greater than all partial degrees of all the polynomials $f_1, \ldots, f_m$. Then the substitution $x_i \mapsto t^{d^{i-1}}$ for all $i \in \{1, \ldots, n\}$ is injective on all monomials appearing in one of $f_1, \ldots, f_m$. This can be used to prove that the polynomials $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$ are F-linearly independent, if and only if the one variable polynomials

$$\varphi_1(t) = f_1(t, t^d, \ldots, t^{d^{n-1}}), \ldots, \varphi_m(t) = f_m(t, t^d, \ldots, t^{d^{n-1}})$$

are F-linearly independent. From Proposition 3.3.3 we know, that this is the case if and only if $W(\varphi_1, \ldots, \varphi_m)$ is not the zero polynomial. But, playing around with derivatives, shows that $W(\varphi_1, \ldots, \varphi_m)$ is an $F[t]$-linear combination of generalized Wronskians

$$W_{\underline{d(1)},\ldots,\underline{d(m)}}(f_1, \ldots, f_m)(t, t^d, \ldots, t^{d^{n-1}})$$

(note that any generalized Wronskian of $f_1, \ldots, f_m$ is an element in $F[x_1, \ldots, x_n]$). We conclude, that if $f_1, \ldots, f_m$ are linearly independent, then at least one generalized Wronskian determinant is not identically zero. This proves the theorem. □

Lemma 3.3.8. *For any $P \in F[x_1, \dots, x_n] \setminus \{0\}$ there are F-linearly independent polynomials $f_0, \dots, f_s \in F[x_1, \dots, x_{n-1}]$, and F-linearly independent polynomials $g_0, \dots, g_s \in F[x_n]$, such that*

$$P(x_1, \dots, x_n) = \sum_{i=0}^{s} f_i(x_1, \dots, x_{n-1}) \cdot g_i(x_n),$$

where $s \leq \deg_{x_n}(P)$.

Proof. Set $\deg_{x_n}(P) = r_n$. We start off by noting that

$$P(x_1, \dots, x_n) = \sum_{i=0}^{r_n} f_i'(x_1, \dots, x_{n-1}) \cdot x^i,$$

for certain $f_0', \dots, f_{r_n}' \in F[x_1, \dots, x_{n-1}]$. The polynomials $1, x_n, \dots, x_n^{r_n}$ are surely F-linearly independent. Hence there is a minimal $s \in \{0, \dots, r_n\}$ such that we can write P in the form

$$P(x_1, \dots, x_n) = \sum_{i=0}^{s} f_i(x_1, \dots, x_{n-1}) \cdot g_i(x_n), \tag{3.14}$$

where $g_0, \dots, g_s \in F[x_n]$ are F-linearly independent. We claim that then also the $f_0, \dots, f_s$ are F-linearly independent. For the sake of contradiction, we assume that the $f_0, \dots, f_s$ are F-linearly dependent. Then, after renumbering the f_i's, we can write

$$f_s = \sum_{i=0}^{s-1} c_i f_i \quad \text{for } c_0, \dots, c_{s-1} \in F.$$

We plug this in into (3.14), which yields

$$P(x_1, \dots, x_n) = \sum_{i=0}^{s-1} f_i(x_1, \dots, x_{n-1}) \cdot (g_i(x_n) + c_i g_s(x_n)).$$

But the polynomials $(g_0(x_n) + c_0 g_s(x_n)), \dots, (g_{s-1}(x_n) + c_{s-1} g_s(x_n))$ are F-linearly independent, since the $g_0, \dots, g_s$ are. This contradicts the minimality of s. Hence, the polynomials $f_0, \dots, f_s$ from (3.14) are indeed F-linearly independent. □

Lemma 3.3.9. *Let $P(x_1, \dots, x_n) = \sum_{i=0}^{s} f_i(x_1, \dots, x_{n-1}) \cdot g_i(x_n) \in F[x_1, \dots, x_n]$ be as in Lemma 3.3.8. Moreover, let $W_{\underline{d(0)}, \dots, \underline{d(s)}}(f_0, \dots, f_s)$ be any generalized Wronskian determinant of $f_0, \dots, f_s$. Then,*

$$W_{\underline{d(0)}, \dots, \underline{d(s)}}(f_0, \dots, f_s) \cdot W_{0,1,\dots,s}(g_0, \dots, g_s) = \det \begin{pmatrix} \partial_{(\underline{d(0)}, 0)} P & \cdots & \partial_{(\underline{d(0)}, s)} P \\ \vdots & \ddots & \vdots \\ \partial_{(\underline{d(s)}, 0)} P & \cdots & \partial_{(\underline{d(s)}, s)} P \end{pmatrix}.$$

Here, for every $i \in \{0, \dots, s\}$ we have $\underline{d(i)} = (d_1(i), \dots, d_{n-1}(i)) \in \mathbb{N}_0^{n-1}$, with $\sum_{j=1}^{n-1} d_j(i) \leq i - 1$, and $(\underline{d(i)}, j) = (d_1(i), \dots, d_s(i), j) \in \mathbb{N}_0^n$ for all $j \in \{0, \dots, n\}$.

Proof. This is essentially a matrix multiplication. We have

$$W_{\underline{d(0)},\dots,\underline{d(s)}}(f_0,\dots,f_s) = \det \underbrace{\begin{pmatrix} \partial_{\underline{d(0)}} f_0 & \cdots & \partial_{\underline{d(0)}} f_s \\ \vdots & \ddots & \vdots \\ \partial_{\underline{d(s)}} f_0 & \cdots & \partial_{\underline{d(s)}} f_s \end{pmatrix}}_{=:W},$$

and (cf. Remark 3.3.6)

$$W_{0,\dots,s}(g_0,\dots,g_s) = \det \begin{pmatrix} \partial_0 g_0 & \cdots & \partial_0 g_s \\ \vdots & \ddots & \vdots \\ \partial_s g_0 & \cdots & \partial_s g_s \end{pmatrix} = \det \underbrace{\begin{pmatrix} \partial_0 g_0 & \cdots & \partial_s g_0 \\ \vdots & \ddots & \vdots \\ \partial_0 g_s & \cdots & \partial_s g_s \end{pmatrix}}_{=:V}.$$

We are left to calculate $W \cdot V$. The entry in line i and row j of $W \cdot V$ is given by

$$\partial_{\underline{d(i)}} f_0 \cdot \partial_j g_0 + \ldots + \partial_{\underline{d(i)}} f_s \cdot \partial_j g_s = \partial_{(\underline{d(i)},j)} f_0 g_0 + \ldots + \partial_{(\underline{d(i)},j)} f_s g_s = \partial_{(\underline{d(i)},j)} P.$$

The first equality comes from the fact that the f_i's are independent on x_n, and the second equality comes from the linearity of the derivation and the definition of P. This proves the lemma. □

Exercises

Exercise 3.5. Fill the gaps in the proof of Theorem 3.3.7. This is: Let $f_1,\dots,f_m \in F[x_1,\dots,x_n]$, where F is a subfield of $\mathbb{C}$, and let $d \in \mathbb{N}$ be greater than $\max_{1\le i\le m, 1\le j\le n} \deg_{x_j}(f_i)$. For all i set

$$\varphi(f_i(x_1,\dots,x_n)) = f_i(t, t^d, \dots, t^{d^{n-1}}) \in F[t],$$

where t is a variable, independent on $x_1,\dots,x_n$.

(a) Prove that the polynomials $f_1,\dots,f_m$ are F-linearly independent, if and only if the polynomials $\varphi(f_1),\dots,\varphi(f_m)$ are linearly independent.

(b) Let $k \in \mathbb{N}_0$ be arbitrary, and set $g^{(k)}$ as the kth derivative of $g \in F[x]$. Prove that there are polynomials $a_{\underline{d},k} \in F[t]$ such that for all $i \in \{1,\dots,m\}$ we have

$$\varphi(f_i)^{(k)} = \sum_{\substack{\partial_{\underline{d}} \\ \operatorname{ord}(\partial_{\underline{d}}) \le k}} a_{\underline{d},k} \partial_{\underline{d}} f_i(t, t^d, \dots, t^{d^{n-1}}).$$

(c) Prove that $W(\varphi(f_1),\dots,\varphi(f_m))$ is a $F[t]$-linear combination of generalized Wronskian determinants of $f_1,\dots,f_m$ evaluated at $(t, t^d, \dots, t^{d^{n-1}})$.

(d) Conclude that some generalized Wronskian determinant of $f_1,\dots,f_m$ is not constantly zero, if the $f_1,\dots,f_m$ are F-linearly independent.

3.4 Preliminaries III – Roth's Lemma

We already know how to construct polynomials of small height that vanish at a given point $\underline{\alpha} \in \overline{\mathbb{Q}}^n$ with large index. The main point in the proof of Roth's theorem is, that we can bound the index of a polynomial at another point $\underline{\beta} \in \overline{\mathbb{Q}}^n$ from above, as long as $\underline{\beta} = (\beta_1, \dots, \beta_n)$ satisfies some properties. Actually, we have to assume that the height of the β_i's is quite large. In our application, the β_i's will be good approximations of a given $\alpha \in \overline{\mathbb{Q}}$ lying in a fixed number field K. If we assume that there are infinitely many such approximations (in order to eventually derive a contradiction), by Northcott' Theorem 2.3.8 there must be approximations of arbitrarily large height. Thus, the assumption of large heights of the β_i's does not cause any difficulties.
Here is the formal result.

Theorem 3.4.1 (Roth's Lemma)**.** *We fix the following data. Let $P \in \overline{\mathbb{Q}}[x_1, \dots, x_n] \setminus \{0\}$ be a polynomial, $\underline{\beta} = (\beta_1, \dots, \beta_n) \in \overline{\mathbb{Q}}^n$ be a point, and let $\sigma \in (0, \frac{1}{2}]$ be a real number. Moreover, we fix $\underline{r} = (r_1, \dots, r_n) \in \mathbb{N}^n$ and assume the following conditions:*

(i) $r_i \geq \deg_{x_i}(P)$ *for all* $i \in \{1, \dots, n\}$,

(ii) $r_{i+1} \leq r_i \cdot \sigma$ *for all* $i \in \{1, \dots, n-1\}$, *and*

(iii) $r_i h(\beta_i) \geq \sigma^{-1}(h_{\mathbb{P}}(P) + 4nr_1)$ *for all* $i \in \{1, \dots, n\}$.

Then, we have $\mathrm{Ind}_{\underline{r},\underline{\beta}}(P) \leq 2n\sigma^{1/2^{n-1}}$.

Remark 3.4.2. These conditions guarantee that the positive integers $r_1, \dots, r_n$ decrease rapidly, and the sequence $h(\beta_1), \dots, h(\beta_n)$ increases rapidly.
Moreover, assumption (i) gives the easy estimate

$$\mathrm{Ind}_{\underline{r},\underline{\beta}}(P) \leq n. \tag{3.15}$$

Hence, Roth's lemma is non-trivial, only if σ is very small.

The rest of this section is devoted to the proof of Theorem 3.4.1. Let us first consider the case $n = 1$, which will actually be our induction base.

Lemma 3.4.3. *Let $P \in \overline{\mathbb{Q}}[x] \setminus \{0\}$, $r \geq \deg(P) \in \mathbb{N}$, and $\beta \in \overline{\mathbb{Q}}$ be arbitrary. Then*

$$\mathrm{Ind}_{r,\beta}(P) \cdot r \cdot h(\beta) = \mathrm{ord}_\beta(P) \cdot h(\beta) \leq h_{\mathbb{P}}(P) + r\log(2).$$

Proof. The first equality sign in the displayed formula is just the definition of the index. By definition of the order, we know that

$$P(x) = (x - \beta)^{\mathrm{ord}_\beta(P)} \cdot P'(x),$$

for some $P'(x) \in \overline{\mathbb{Q}}[x]$ with $P'(\beta) \neq 0$. Hence

$$h_{\mathbb{P}}(P) \overset{3.2.12}{\geq} -\deg(P)\log(2) + h_{\mathbb{P}}((x-\beta)^{\mathrm{ord}_\beta(P)}) + h_{\mathbb{P}}(P') \geq -r\log(2) + \mathrm{ord}_\beta(P)h(\beta),$$

which proves the lemma. For the last inequality, we have used $r \geq \deg(P)$, $h_{\mathbb{P}}(P') \geq 0$, and

$$\begin{aligned}
h_{\mathbb{P}}((x-\beta)^{\mathrm{ord}_\beta(P)}) &= h_{\mathbb{P}}\left(\sum_{i=0}^{\mathrm{ord}_\beta(P)} \binom{\mathrm{ord}_\beta(P)}{i}(-\beta)^i x^{\mathrm{ord}_\beta(P)-i}\right) \\
&= \frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]} \sum_{v\in M_{\mathbb{Q}(\beta)}} d_v \log\left(\max_{0\leq i\leq \mathrm{ord}_\beta(P)} \left|\binom{\mathrm{ord}_\beta(P)}{i}\beta^i\right|_v\right) \\
&\geq \frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]} \sum_{v\in M_{\mathbb{Q}(\beta)}} d_v \log\left(\max_{i\in\{0,\mathrm{ord}_\beta(P)\}} \left|\binom{\mathrm{ord}_\beta(P)}{i}\beta^i\right|_v\right) \\
&= \frac{1}{[\mathbb{Q}(\beta):\mathbb{Q}]} \sum_{v\in M_{\mathbb{Q}(\beta)}} d_v \log\left(\max\{1, \left|\beta^{\mathrm{ord}_\beta(P)}\right|_v\}\right) \\
&= h(\beta^{\mathrm{ord}_\beta(P)}) = \mathrm{ord}_\beta(P)h(\beta).
\end{aligned}$$

□

Remark 3.4.4. If $r \in \mathbb{N}$ and $\beta \in \overline{\mathbb{Q}}$ satisfy assumption (iii) from Roth's Lemma 3.4.1 (which just means $rh(\beta) \geq \sigma^{-1}(h_{\mathbb{P}}(P) + 4r)$), then Lemma 3.4.3 implies

$$\mathrm{Ind}_{r,\beta}(P) \leq \sigma \cdot \left(\frac{h_{\mathbb{P}}(P) + r\log(2)}{h_{\mathbb{P}}(P) + 4r}\right) \leq \sigma < 2\sigma,$$

which indeed proves Roth's Lemma 3.4.1 for $n = 1$.

From now on we use the notation from Roth's Lemma 3.4.1, and assume (as our induction hypothesis) that the statement is correct for all natural numbers $< n$.

3.4.5. We apply Lemma 3.3.8 to write

$$P(x_1,\ldots,x_n) = \sum_{i=0}^{s} f_i(x_1,\ldots,x_{n-1})\cdot g_i(x_n),$$

with $s \leq \deg_{x_n}(P) \leq r_n$, and $f_0,\ldots,f_s \in \overline{\mathbb{Q}}[x_1,\ldots,x_{n-1}]$ are ($\overline{\mathbb{Q}}$-)linearly independent, and $g_0,\ldots,g_s \in \overline{\mathbb{Q}}[x_n]$ are also linearly independent.
By Theorem 3.3.7 there is a generalized Wronskian determinant

$$U(x_1,\ldots,x_{n-1}) := W_{\underline{d(0)},\ldots,\underline{d(s)}}(f_0,\ldots,f_s) \in \overline{\mathbb{Q}}[x_1,\ldots,x_{n-1}] \setminus \{0\},$$

and as well it is

$$V(x_n) := W_{0,\ldots,s}(g_0,\ldots,g_s) \in \overline{\mathbb{Q}}[x_n] \setminus \{0\}.$$

We apply Lemma 3.3.9 to conclude that

$$W(x_1,\ldots,x_n) = \det\begin{pmatrix} \partial_{(\underline{d(0)},0)}P & \cdots & \partial_{(\underline{d(0)},s)}P \\ \vdots & \ddots & \vdots \\ \partial_{(\underline{d(s)},0)}P & \cdots & \partial_{(\underline{d(s)},s)}P \end{pmatrix} \in \overline{\mathbb{Q}}[x_1,\ldots,x_n] \setminus \{0\}.$$

Since the partial degree at x_i of any entry in the above matrix is bounded from above by $\deg_{x_i}(P) \leq r_i$ for all $i \in \{1,\ldots,n\}$, we conclude

$$\deg_{x_i}(W) \leq r_i(s+1) \quad \forall\, i \in \{1,\ldots,n\}, \tag{3.16}$$

and in particular, $\deg_{x_i}(U) \leq r_i(s+1)$ for all $i \in \{1,\ldots,n-1\}$, and $\deg_{x_n}(V) \leq r_n(s+1)$.

We aim to apply our induction hypothesis to the polynomials U and V. For all $i \in \{1, \dots, n\}$ we set $r_i' = r_i(s+1)$. We have just seen, that U and V satisfy assumption (i) from Roth's Lemma, with r_i replaced by r_i'. Moreover, since $r_1, \dots, r_n$ satisfy assumption (ii), also $r_1', \dots, r_n'$ satisfy assumption (ii). We need to show that U and V, together with the natural numbers $r_1', \dots, r_n'$ also satisfy assumption (iii). This is, we need

$$(s+1)r_i h(\beta_i) \geq \sigma^{-1}(h_{\mathbb{P}}(U) + 4(n-1)r_1(s+1)) \quad \forall\, i \in \{1, \dots, n-1\}, \tag{3.17}$$

and

$$(s+1)r_n h(\beta_n) \geq \sigma^{-1}(h_{\mathbb{P}}(V) + 4r_n(s+1)). \tag{3.18}$$

Since we assume that $r_i h(\beta_i) \geq \sigma^{-1}(h_{\mathbb{P}}(P) + 4nr_1)$ for all $i \in \{1, \dots, n\}$ (and $r_n < r_1$), the inequalities (3.18) and (3.17) follow as soon as we know $h_{\mathbb{P}}(U) \leq (s+1)(h_{\mathbb{P}}(P) + 4r_1)$, and $h_{\mathbb{P}}(V) \leq (s+1)(h_{\mathbb{P}}(P) + 4r_1)$. This is what we are going to prove now. More precisely, we will prove

$$h_{\mathbb{P}}(U) + h_{\mathbb{P}}(V) = h_{\mathbb{P}}(W) \leq (s+1)(h_{\mathbb{P}}(P) + 4r_1), \tag{3.19}$$

where the equality sign, was proven in the exercise sessions, as U and V are defined over independent variables.

3.4.6. We write S_{s+1} for the set of bijections of the set $\{0, \dots, s\}$. Then, by the Leibniz formula, we have

$$W(x_1, \dots, x_n) = \sum_{\pi \in S_{s+1}} \operatorname{sign}(\pi) \prod_{i=0}^{s} \partial_{\underline{(d(i)}, \pi(i))} P. \tag{3.20}$$

Let K be any number field containing all coefficients of P. Note that the sum of two polynomials is defined coefficient-wise. Hence, the absolute values on polynomials satisfy the usual (ultrametric) triangular inequalities. Hence, as seen many times before, we have

$$\begin{aligned}\left| \sum_{\pi \in S_{s+1}} \operatorname{sign}(\pi) \prod_{i=0}^{s} \partial_{\underline{(d(i)}, \pi(i))} P \right|_v &\leq \max_{\pi \in S_{s+1}} \left| \prod_{i=0}^{s} \partial_{\underline{(d(i)}, \pi(i))} P \right|_v \\ &\overset{2.3.2}{=} \max_{\pi \in S_{s+1}} \prod_{i=0}^{s} \left| \partial_{\underline{(d(i)}, \pi(i))} P \right|_v,\end{aligned}$$

if $v \in M_K$ is non-archimedean, and

$$\begin{aligned}\left| \sum_{\pi \in S_{s+1}} \operatorname{sign}(\pi) \prod_{i=0}^{s} \partial_{\underline{(d(i)}, \pi(i))} P \right|_v &\leq \underbrace{(s+1)!}_{=|S_{s+1}|} \max_{\pi \in S_{s+1}} \left| \prod_{i=0}^{s} \partial_{\underline{(d(i)}, \pi(i))} P \right|_v \\ &\overset{3.2.11}{\leq} (s+1)! 2^{r_1 + \dots + r_n} \max_{\pi \in S_{s+1}} \prod_{i=0}^{s} \left| \partial_{\underline{(d(i)}, \pi(i))} P \right|_v,\end{aligned}$$

if $v \in M_K$ is archimedean. Luckily, the definition of $\partial_{\underline{(d(i)}, \pi(i))} P$ (see also (2.34)) gives us readily the estimates

$$\left| \partial_{\underline{(d(i)}, \pi(i))} P \right|_v \leq \begin{cases} |P|_v & \text{, if } v \text{ is non-archimedean} \\ 2^{r_1 + \dots + r_n} |P|_v & \text{, if } v \text{ is archimedean.} \end{cases}$$

For the archimedean estimate we have used – as in (2.38) – the estimates $\binom{i}{d} \leq 2^i \leq 2^r$ for all $i \leq r$. We combine all these estimates to achieve

$$\begin{aligned} h_{\mathbb{P}}(W) &\leq (s+1)h_{\mathbb{P}}(P) + \log(2^{(s+1)(r_1+\ldots+r_n)}) + \log(2^{r_1+\ldots+r_n}) + \log((s+1)!) \\ &= (s+1)h_{\mathbb{P}}(P) + (s+2)(r_1+\ldots+r_n)\log(2) + \log((s+1)!) \\ &= (s+1)(h_{\mathbb{P}}(P) + \frac{(s+2)(r_1+\ldots+r_n)\log(2)}{s+1} + \frac{\log((s+1)!)}{s+1}) \\ &\leq (s+1)(h_{\mathbb{P}}(P) + 2(r_1+\ldots+r_n)\log(2) + \frac{\log((s+1)!)}{s+1}) \end{aligned} \tag{3.21}$$

Assumption (ii) of Roth's Lemma 3.4.1 gives the estimate $r_1 + \ldots + r_n \leq 2r_1$, and a trivial induction shows $\log((s+1)!) \leq (s+1)\cdot\log(s+1) \leq (s+1)\log(r_n+1) \leq (s+1)r_n$. Moreover, again by assumption (ii), it is $r_n \leq \frac{1}{2}r_1$. Throwing these estimates into (3.21) proves (3.19).

Now we can apply our induction hypothesis for $U \in \overline{\mathbb{Q}}[x_1,\ldots,x_{n-1}] \subseteq \overline{\mathbb{Q}}[x_1,\ldots,x_n]$, $\underline{r'} = ((s+1)r_1,\ldots,(s+1)r_n)$, and $\underline{\beta} = (\beta_1,\ldots,\beta_n)$. This is, we can conclude that

$$\mathrm{Ind}_{\underline{r},\underline{\beta}}(U) = (s+1)\,\mathrm{Ind}_{\underline{r'},\underline{\beta}}(U) \leq 2(s+1)(n-1)\sigma^{1/2^{n-2}}.$$

Here we have used that, since x_n does not appear in U, the index $\mathrm{Ind}_{\underline{r'},\underline{\beta}}(U)$ is the same as removing the last entry in $\underline{r'}$ and in $\underline{\beta}$. Hence, this is indeed the induction hypothesis. Applying the same argument for V and Lemma 3.4.3 gives

$$\mathrm{Ind}_{\underline{r},\underline{\beta}}(V) = (s+1)\,\mathrm{Ind}_{\underline{r'},\underline{\beta}}(V) \leq (s+1)\sigma$$

(cf. Remark 3.4.4). As seen in the exercises, the index behaves well under multiplication of polynomials. Hence, we conclude

$$\mathrm{Ind}_{\underline{r},\underline{\beta}}(W) = \mathrm{Ind}_{\underline{r},\underline{\beta}}(U) + \mathrm{Ind}_{\underline{r},\underline{\beta}}(V) \leq 2(s+1)(n-1)\sigma^{1/2^{n-2}} + (s+1)\sigma. \tag{3.22}$$

We have bounded the index of W, so all that is left to do is to compare the index of W with the index of P. Since W was constructed in terms of P, this should be possible.

3.4.7. The index of a polynomial also satisfies a "logarithmic ultrametric triangular equation". This is, for any $f, g \in \overline{\mathbb{Q}}[x_1,\ldots,x_n]$ we have

$$\mathrm{Ind}_{\underline{r},\underline{\beta}}(f+g) \geq \min\{\mathrm{Ind}_{\underline{r},\underline{\beta}}(f), \mathrm{Ind}_{\underline{r},\underline{\beta}}(g)\}.$$

We have seen this in the case $n = 1$ in the exercises. The general statement follows similarly. Using (3.20), we conclude

$$\mathrm{Ind}_{\underline{r},\underline{\beta}}(W) \geq \min_{\pi\in S_{s+1}} \left\{ \sum_{i=0}^{s} \mathrm{Ind}_{\underline{r},\underline{\beta}}(\partial_{(\underline{d(i)},\pi(i))}P) \right\}. \tag{3.23}$$

The $\partial_{\underline{d(i)}}$ was part of a generalized Wronskian determinant. Therefore, writing $\underline{d(i)} = (d_1(i),\ldots,d_{n-1}(i))$, we have $d_1(i) + \ldots + d_{n-1}(i) \leq i - 1 \leq (s+1) - 1 = s \leq r_n$. Moreover, $r_1 > r_2 > \ldots > r_n > 0$, and $r_n/r_{n-1} \leq \sigma$ by assumption (ii) of Roth's Lemma 3.4.1. Now,

(almost) from the definition of the index, we have

$$\begin{aligned}\operatorname{Ind}_{\underline{r},\underline{\beta}}(\partial_{\underline{(d(i),\pi(i))}}P) &\geq \operatorname{Ind}_{\underline{r},\underline{\beta}}(P) - \frac{d_1(i)}{r_1} - \ldots - \frac{d_{n-1}(i)}{r_{n-1}} - \frac{\pi(i)}{r_n} \\ &\geq \operatorname{Ind}_{\underline{r},\underline{\beta}}(P) - \frac{0}{r_1} - \ldots - \frac{0}{r_{n-2}} - \frac{i-1}{r_{n-1}} - \frac{\pi(i)}{r_n} \\ &\geq \operatorname{Ind}_{\underline{r},\underline{\beta}}(P) - \frac{r_n}{r_{n-1}} - \frac{\pi(i)}{r_n} \\ &\geq \operatorname{Ind}_{\underline{r},\underline{\beta}}(P) - \frac{\pi(i)}{r_n} - \sigma\end{aligned}$$

Since the index is never negative, we can replace this estimate by

$$\operatorname{Ind}_{\underline{r},\underline{\beta}}(\partial_{\underline{(d(i),\pi(i))}}P) \geq \max\{\operatorname{Ind}_{\underline{r},\underline{\beta}}(P) - \frac{\pi(i)}{r_n} - \sigma, 0\} \geq \max\{\operatorname{Ind}_{\underline{r},\underline{\beta}}(P) - \frac{\pi(i)}{r_n}, 0\} - \sigma \quad (3.24)$$

for all $i \in \{0, \ldots, s\}$. The last technicality that we will need is the following lemma.

Lemma 3.4.8. *Let $k \in \mathbb{N}_0$ and $\delta \in \mathbb{R}$ be arbitrary, then*

$$\sum_{i=0}^{k} \max\{\delta - \frac{i}{k}, 0\} \geq (k+1) \cdot \min\{\frac{1}{2}\delta, \frac{1}{2}\delta^2\}.$$

Now, we have

$$\begin{aligned}\operatorname{Ind}_{\underline{r},\underline{\beta}}(W) &\overset{(3.23)}{\geq} \min_{\pi \in S_{s+1}} \left\{ \sum_{i=0}^{s} \operatorname{Ind}_{\underline{r},\underline{\beta}}(\partial_{\underline{(d(i),\pi(i))}}P) \right\} \\ &\overset{(3.24)}{\geq} \min_{\pi \in S_{s+1}} \left\{ \sum_{i=0}^{s} \left(\max\{\operatorname{Ind}_{\underline{r},\underline{\beta}}(P) - \frac{\pi(i)}{r_n}, 0\} - \sigma \right) \right\} \\ &= \sum_{i=0}^{s} \left(\max\{\operatorname{Ind}_{\underline{r},\underline{\beta}}(P) - \frac{i}{r_n}, 0\} \right) - (s+1)\sigma \\ &\overset{3.4.8}{\geq} (s+1) \min\{\frac{1}{2}\operatorname{Ind}_{\underline{r},\underline{\beta}}(P), \frac{1}{2}\operatorname{Ind}_{\underline{r},\underline{\beta}}(P)^2\} - (s+1)\sigma. \qquad (3.25)\end{aligned}$$

We are almost done! Comparing the upper bound (3.22) with the lower bound (3.25), gives

$$\begin{aligned}& 2(n-1)\sigma^{1/2^{n-2}} + \sigma \geq \min\{\frac{1}{2}\operatorname{Ind}_{\underline{r},\underline{\beta}}(P), \frac{1}{2}\operatorname{Ind}_{\underline{r},\underline{\beta}}(P)^2\} - \sigma \\ \implies\quad & 4(n-1)\sigma^{1/2^{n-2}} + 4\sigma \geq \min\{\operatorname{Ind}_{\underline{r},\underline{\beta}}(P), \operatorname{Ind}_{\underline{r},\underline{\beta}}(P)^2\}\end{aligned}$$

Thus, we have

$$\operatorname{Ind}_{\underline{r},\underline{\beta}}(P)^2 \leq 4(n-1)\sigma^{1/2^{n-2}} + 4\sigma,$$

or

$$\operatorname{Ind}_{\underline{r},\underline{\beta}}(P)^2 \overset{(3.15)}{\leq} n \operatorname{Ind}_{\underline{r},\underline{\beta}}(P) \leq 4n(n-1)\sigma^{1/2^{n-2}} + 4n \underbrace{\sigma}_{\leq \sigma^{1/2^{n-2}}}.$$

So, this latter estimate holds in any case. Taking the square root gives

$$\operatorname{Ind}_{\underline{r},\underline{\beta}}(P) \leq \left(4n(n-1)\sigma^{1/2^{n-2}} + 4n\sigma^{1/2^{n-2}}\right)^{1/2} = 2n\sigma^{1/2^{n-1}},$$

proving Roth's Lemma 3.4.1.

Exercises

Exercise 3.6. Let $F \subseteq \mathbb{C}$ be a field, and let $F[x_1, \dots, x_n]$ be the polynomial ring in n variables over F. Moreover, let $\underline{r} \in \mathbb{N}^n$ and $\underline{\beta} \in F^n$ be arbitrary. Prove that for all $f, g \in F[x_1, \dots, x_n]$ we have

$$\mathrm{Ind}_{\underline{r},\underline{\beta}}(f+g) \geq \min\{\mathrm{Ind}_{\underline{r},\underline{\beta}}(f), \mathrm{Ind}_{\underline{r},\underline{\beta}}(g)\}.$$

Exercise 3.7. Let $k \in \mathbb{N}_0$ and $\delta \in \mathbb{R}$ be arbitrary. Prove that

$$\sum_{i=0}^{k} \max\{\delta - \frac{i}{k}, 0\} \geq (k+1) \cdot \min\{\frac{1}{2}\delta, \frac{1}{2}\delta^2\}.$$

3.5 The Proof

Now, we will finally prove Roth's Theorem. We will follow the outline from [1].

Roth's Theorem 3.0.1. *Let K be a number field of degree d, and let $S \subseteq M_K$ be finite. For any $\alpha \in \overline{\mathbb{Q}}$ and for each element $v \in M_K$ we fix one extension $v' \mid v$ to $K(\alpha)$. Then, for all $\varepsilon > 0$ there are at most finitely many $\beta \in K$ such that*

$$\prod_{v \in S} \min\{1, |\alpha - \beta|_{v'}\}^{d_v} < H(\beta)^{-d(2+\varepsilon)}.$$

Remark 3.5.1. To ease notation, we will replace $2 + \varepsilon$, for some $\varepsilon > 0$, by an $\kappa > 2$ (I only introduce a new variable κ, since writing "let $\varepsilon > 2$ ..." sounds like a bad math-joke.)

From now on, we assume that there are infinitely many $\beta \in K$ satisfying

$$\prod_{v \in S} \min\{|\alpha - \beta|_{v'}, 1\}^{d_v} \leq \frac{1}{H(\beta)^{d\kappa}}, \tag{3.26}$$

for some fixed $\kappa > 2$. This will eventually lead to a contradiction.

3.5.1 Comparing Different Approximations

The first difficulty arises right away from allowing more then one absolute value. This enables good approximations of the same α to have arithmetically nothing in common.

Example 3.5.2. Let $\alpha = \sqrt{17}$, $K = \mathbb{Q}$, and $S = \{\infty, 2\}$. We remark, that $\sqrt{17}$ is in $\mathbb{Q}_2$. Hence, there are good 2-adic approximations of $\sqrt{17}$. If our α would not be in $\mathbb{Q}_2$, the information that $2 \in S$ would be irrelevant (see Remark 3.0.3).
The fact that $\sqrt{17} \in \mathbb{Q}_2$ means that the ideal $2\mathcal{O}_{\mathbb{Q}(\sqrt{17})}$ splits into two different prime ideals. Luckily, $\mathcal{O}_{\mathbb{Q}(\sqrt{17})} = 1 \cdot \mathbb{Z} + \frac{1+\sqrt{17}}{2} \cdot \mathbb{Z}$ is a principle ideal domain, and hence factorial. The element $\frac{\sqrt{17}-5}{2}$ has norm 2. Therefore, the ideal generated by this element is a prime ideal, and the associated absolute value is an extension of $|.|_2$ – hence it takes the role of $2'$. For ∞' we take the usual archimedean absolute value on $\mathbb{Q}(\sqrt{17})$.
We give three examples of approximations of α:

- $\left|\sqrt{17}-4\right|_{\infty'} = 0,1231\ldots$, and $\left|\sqrt{17}-4\right|_{2'} = 1$ (the norm of this element is odd, and hence, it has nothing to do with our chosen prime ideal).
- $\left|\sqrt{17}-1\right|_{\infty'} = 3,1231\ldots$, and

$$\left|\sqrt{17}-1\right|_{2'} = \left|\left(\frac{\sqrt{17}-5}{2}\right)^3 \cdot \left(\frac{-37-9\sqrt{17}}{2}\right)\right|_{2'} = \left(\frac{1}{2}\right)^3.$$

- $\left|\sqrt{17}-\frac{433}{105}\right|_{\infty'} = 0,00073\ldots$, and

$$\left|\sqrt{17}-\frac{433}{105}\right|_{2'} = \left|\frac{2}{105}\cdot\left(\frac{\sqrt{17}-5}{2}\right)^4\right|_{2'} = |2|_2 \cdot \left|\frac{\sqrt{17}-5}{2}\right|_{2'}^4 = \left(\frac{1}{2}\right)^5.$$

In all cases $\prod_{v\in\{\infty,2\}} \min\{\left|\sqrt{17}-\beta\right|_{v'}^{d_v}, 1\} < 1$, but somehow the reason why the product is less than 1 is different in all three cases. One could say, that the approximations lie in different *approximation classes*. We will make this precise in the following.

Definition 3.5.3. A $\beta \in K$ is called *non-trivial approximation* if

$$\Lambda(\beta) = \prod_{v\in S} \min\{|\alpha-\beta|_{v'}, 1\}^{d_v} < 1.$$

The set of non-trivial approximations different from α will be denoted with $B = \{\beta \in K | 0 \neq \Lambda(\beta) < 1\}$.

We recall, that everything in this section, will depend on our fixed data α, S, and K.
We consider the map

$$L : B \longrightarrow (0,1]^{|S|} \quad ; \quad \beta \mapsto \left(\frac{\log(\min\{1, |\alpha-\beta|_{v'}^{d_v}\})}{\log(\Lambda(\beta))}\right)_{v\in S}.$$

This map is well defined by the definition of $\Lambda(\beta)$ and B. For any $N \in \mathbb{N}$, we cut the cube $(0,1]^{|S|}$ into subcubes of side-length $\frac{1}{N}$. More precisely, for all $(i_v)_{v\in S} \in \{0,1,\ldots,N-1\}^{|S|}$ we define

$$I((i_v)_{v\in S}) = \prod_{v\in S} (\frac{i_v}{N}, \frac{i_v+1}{N}] \subseteq (0,1]^{|S|}.$$

Definition 3.5.4. For all $N \in \mathbb{N}$, and $(i_v)_{v\in S} \in \{0,\ldots,N-1\}^{|S|}$ we set

$$\mathcal{C}(N,(i_v)_{v\in S}) = \{\beta \in B | L(\beta) \in I((i_v)_{v\in S})\},$$

and call this an *approximation class of size* $1/N$.

Lemma 3.5.5. *Let $N \in \mathbb{N}$ and $(i_v)_{v\in S} \in \{0,\ldots,N-1\}^{|S|}$ be as above. If there is some $\beta \in \mathcal{C}(N,(i_v)_{v\in S})$, then*

(i) $\Lambda(\beta)^{(i_v+1)/N} < \min\{1, |\alpha-\beta|_{v'}^{d_v}\} \leq \Lambda(\beta)^{i_v/N}$ *for all $v \in S$, and*

(ii) $1 - \frac{|S|}{N} \leq \sum_{v \in S} \frac{i_v}{N} \leq 1$.

Proof. By definition of the approximation class $\mathcal{C}(N, (i_v)_{v \in S})$, we have for all $v \in S$

$$\frac{i_v}{N} \leq \frac{\log(\min\{1, |\alpha - \beta|_{v'}^{d_v}\})}{\log(\Lambda(\beta))} < \frac{i_v + 1}{N}. \tag{3.27}$$

Since $\log(\Lambda(\beta))$ is always negative, this is equivalent to

$$\frac{i_v}{N} \log(\Lambda(\beta)) \geq \log(\min\{1, |\alpha - \beta|_{v'}^{d_v}\}) > \frac{i_v + 1}{N} \log(\Lambda(\beta)).$$

Applying the exponential function proves part (i). By definition of $\Lambda(\beta)$, we have that the sum over all $v \in S$ of the middle term in (3.27) is equal to 1. Hence, summing up (3.27) over all $v \in S$ gives

$$\sum_{v \in S} \frac{i_v}{N} \leq 1 \leq \sum_{v \in S} \frac{i_v + 1}{N} = \frac{|S|}{N} + \sum_{v \in S} \frac{i_v}{N}.$$

This proves part also (ii). □

For any $N \in \mathbb{N}$ there are only finitely many approximation classes of size $1/N$. Hence, by the box principle, we know for all N there is an $\mathcal{C}(N, (i_v)_{v \in S})$ containing infinitely many β which satisfy (3.26). This means, that we can restrict to approximations of α of the same type. By Northcott's Theorem 2.3.8, among these infinitely many β's there are elements of arbitrary large height.

3.5.6. Hence, for all $n, L, M, N \in \mathbb{N}$ there are $\beta_1, \ldots, \beta_n$ satisfying (3.26), such that

(A) $\beta_1, \ldots, \beta_n$ lie in the same approximation class $\mathcal{C}(N, (i_v)_{v \in S})$ of size $1/N$,

(B) $h(\beta_1) \geq L$, and

(C) $h(\beta_{i+1}) \geq M h(\beta_i)$ for all $i \in \{1, \ldots, n-1\}$.

Throughout the proof, we need to collect some restrictions on these (and other) constants. At the end, we have to choose the constants such that we derive a contradiction. Part (C) should remind you on the assumptions of Roth's Lemma 3.4.1. In order to be able to apply Roth's Lemma, our first restriction is

(C') $M \geq 2$.

Applying these assumptions, gives in particular

$$\sum_{j=1}^{n} \frac{1}{h(\beta_j)} \leq \sum_{j=1}^{n} \frac{1}{LM^{j-1}} \leq \sum_{j=0}^{\infty} \frac{1}{LM^j} = \frac{1}{L} \left(\frac{M}{M-1} \right) \leq \frac{2}{L}, \tag{3.28}$$

and hence for any $D \in \mathbb{N}$

$$\sum_{j=1}^{n} \left\lfloor \frac{D}{h(\beta_j)} \right\rfloor \leq D \sum_{j=1}^{n} \frac{1}{h(\beta_j)} \leq \frac{2D}{L}. \tag{3.29}$$

3.5.2 Construction of the Polynomial

As noted several times before, we aim to use an auxiliary polynomial. This was constructed in Theorem 2.6.5. Looking into the assumptions of this theorem, we see that we need an $\varepsilon \in (0,1)$, and we need to bound the local degrees of the polynomial that we want to construct.

(D) We choose a real number $\varepsilon \in (0, 1/2)$, and assume that $n > \frac{4\log(2[\mathbb{Q}(\alpha):\mathbb{Q}])}{\varepsilon^2}$.

(E) For some $D > h(\beta_n)$ we set $r_i = \lfloor D/h(\beta_i) \rfloor$ for all $i \in \{1, \dots, n\}$.

Then by Theorem 2.6.5, there exists a polynomial $P \in \mathbb{Z}[x_1, \dots, x_n] \setminus \{0\}$ such that

- $\deg_{x_i}(P) \leq r_i$ for all $i \in \{1, \dots, n\}$,
- $\mathrm{Ind}_{(\underline{\alpha},\underline{r})}(P) \geq \frac{n}{2}(1-\varepsilon)$ where $\underline{\alpha} = (\alpha, \dots, \alpha)$, and
- $h_{\mathbb{P}}(P) \leq \left(\sum_{j=1}^n r_j\right)(\log(4) + h(\alpha)) \overset{(3.29)}{\leq} \frac{2D}{L} \underbrace{(\log(4) + h(\alpha))}_{=C_1}$.

In the formulation of Theorem 2.6.5 we have an estimate for $h(P)$ instead of $h_{\mathbb{P}}(P)$. But we can safely assume that the coefficients of P are coprime, and in that case we have $h(P) = h_{\mathbb{P}}(P)$. Next, we want to apply Roth's Lemma 3.4.1. To do this, we have to check the assumptions. Hence, let $\sigma \in (0,1)$ be a real number. We start with $r_{i+1} \leq r_i\sigma$ for all $i \in \{1, \dots, n-1\}$. Roughly, r_i is almost equal to $D/h(\beta_i)$, and asymptotically this statement becomes more and more precise, with increasing D. So we should think of D as a very large integer. With $r_i \approx \frac{D}{h(\beta_i)}$, we find that in order to verify $r_{i+1} \leq r_i\sigma$, we should assume $M > \sigma^{-1}$. To keep things simple, we thus assume

$$M \geq 2\sigma^{-1}.$$

If D is large enough to satisfy

$$\frac{D}{D - h(\beta_i)} \leq 2 \quad \forall\, i \in \{1, \dots, n\},$$

then for all $i \in \{1, \dots, n-1\}$, our choice of M implies

$$\begin{aligned} & \frac{D}{M(D-h(\beta_i))} \leq \sigma \quad \overset{(C)}{\Longrightarrow} \quad \frac{Dh(\beta_i)}{h(\beta_{i+1})(D-h(\beta_i))} \leq \sigma \\ \Longleftrightarrow \quad & \frac{D}{h(\beta_{i+1})} \leq \sigma \cdot \left(\frac{D}{h(\beta_i)} - 1\right) \quad \Longrightarrow \quad \underbrace{\lfloor D/h(\beta_{i+1}) \rfloor}_{=r_{i+1}} \leq \sigma \cdot \underbrace{\lfloor D/h(\beta_i) \rfloor}_{=r_i}. \end{aligned}$$

Similarly, if D is large enough to satisfy

$$\frac{D}{D - h(\beta_i)} \leq \frac{5}{4} \quad \forall\, i \in \{1, \dots, n\}, \tag{3.30}$$

then

$$L \geq \sigma^{-1} \cdot (\frac{5}{2}C_1 + 5n)$$

implies $r_i h(\beta_i) \geq \sigma^{-1}(h_{\mathbb{P}}(P) + 4nr_1)$ for all $i \in \{1, \ldots, n\}$. Now we can indeed apply Roth's Lemma 3.4.1, and we conclude that $\mathrm{Ind}_{(\underline{\beta},\underline{r})}(P) \leq 2n\sigma^{1/2^{n-1}}$. This means, that for some $\partial_{\underline{d}}$, with

$$\frac{d_1}{r_1} + \ldots + \frac{d_n}{r_n} \leq 2n\sigma^{1/2^{n-1}}, \tag{3.31}$$

we have $\partial_{\underline{d}} P(\underline{\beta}) \neq 0$. Moreover, we conclude

$$\mathrm{Ind}_{(\underline{\alpha},\underline{r})}(\partial_{\underline{d}} P) \geq \mathrm{Ind}_{(\underline{\alpha},\underline{r})}(P) - 2n\sigma^{1/2^{n-1}}. \tag{3.32}$$

We want that this index is still "large". Therefore, we fix $\sigma = (\varepsilon\frac{5}{4})^{2^{n-1}}$, which leads to the following estimates for M and L:

(F) $M \geq 2 \cdot \left(\varepsilon\frac{5}{4}\right)^{-2^{n-1}}$, and

(G) $L \geq (\varepsilon\frac{5}{4})^{-2^{n-1}} \cdot (\frac{5}{2}C_1 + 5n)$.

Under these assumptions, we get:

Lemma 3.5.7. *For all $D \in \mathbb{N}$ satisfying*

(H) $D \geq 5h(\beta_n)$

there exists a polynomial $Q \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

(i) $\deg_{x_i}(Q) \leq r_i$ *for all* $i \in \{1, \ldots, n\}$,

(ii) $\mathrm{Ind}_{(\underline{\alpha},\underline{r})}(Q) \geq (\frac{1}{2} - 3\varepsilon)n$,

(iii) $Q(\underline{\beta}) \neq 0$, *and*

(iv) $h_{\mathbb{P}}(Q) \leq 4C_1\frac{D}{L}$.

Proof. First we note that condition (H) implies (3.30). We set $Q = \partial_{\underline{d}} P$, with $\underline{d}$ as in (3.31). Then we immediately see that (i) and (iii) are satisfied. Moreover, we know that $\mathrm{Ind}_{(\underline{\alpha},\underline{r})}(P) \geq \frac{n}{2}(1-\varepsilon)$, and $\sigma = (\varepsilon\frac{5}{4})^{2^{n-1}}$. Plugging this into (3.32) gives (ii). By the Leibniz rule (cf. (2.34)), we know that the coefficients of Q are increased compared to the coefficients of P at most by a factor of $\prod_{i=1}^{n} \binom{r_i}{\lfloor r_i/2 \rfloor} < 2^{r_1+\ldots+r_n} \overset{(3.29)}{\leq} 2^{2D/L}$. Hence,

$$h_{\mathbb{P}}(Q) \leq \log(2^{2D/L}) + h_{\mathbb{P}}(P) \leq \frac{2D}{L}\log(2) + \underbrace{C_1}_{\geq \log(2)} \frac{2D}{L} \leq 4C_1\frac{2D}{L},$$

proving the lemma. □

3.5.3 Bounding the Size of the Polynomial Value

We want to measure the "size" of the non-negative value $Q(\underline{\beta})$. We will do this, by estimating $\sum_{v \in M_K} d_v \log(\left|Q(\underline{\beta})\right|_v)$. Since $Q(\underline{\beta}) \neq 0$, the product formula 2.2.16 gives us the precise value, namely

$$\sum_{v \in M_K} d_v \log(\left|Q(\underline{\beta})\right|_v) = 0. \tag{3.33}$$

The aim is to find a contradiction to this equality.
For any $v \in M_K$ the maximum of all summands in the representation of $Q(\underline{\beta})$ is less then $|Q|_v \cdot \prod_{j=1}^n \max\{1, |\beta_j|_v\}^{\deg_{x_j}(Q)}$. Moreover, there are at most $\prod_{j=1}^n (\deg_{x_j}(Q)+1)$ summands. Since $\deg_{x_j}(Q) \leq r_j$ for all $j \in \{1, \dots, n\}$ we conclude that

$$\log(\left|Q(\underline{\beta})\right|_v) \leq \log(|Q|_v) + \sum_{j=1}^n r_j \left(\log(\max\{1, |b_j|_v\}) + \delta_v \frac{\log(r_j+1)}{r_j}\right) \quad \forall\, v \in M_K, \quad (3.34)$$

where

$$\delta_v = \begin{cases} 0 & \text{if } v \nmid \infty \\ 1 & \text{if } v \mid \infty. \end{cases}$$

Next, we are going to improve this bound for all $v \in S$. Hence, from now on we will assume

$$v \in S.$$

Keep in mind, that vaguely spoken the β_j's are chosen such that $|\alpha - \beta_j|_v$ is small. Hence, we want to represent $Q(\underline{\beta})$ using terms of the form $\alpha - \beta_j$. But there is a well-known way to do this. We just use the Taylor expansion of Q centred at $\underline{\alpha}$. Since our differential operators $\partial_{\underline{d}}$ already take care of the correct normalization. This Taylor expansion reads

$$Q(\underline{\beta}) = \sum_{\underline{d} \in \mathbb{N}_0^n} \partial_{\underline{d}} Q(\underline{\alpha})(\alpha - \beta_1)^{d_1} \cdots (\alpha - \beta_n)^{d_n}. \quad (3.35)$$

We have to estimate two things. First we will estimate $\left|\partial_{\underline{d}} Q(\underline{\alpha})\right|_{v'}$, and then we will use our assumption (3.26) to estimate the v'-absolute value of the other factors. By construction of Q (see Lemma 3.5.7), we have

$$\partial_{\underline{d}} Q(\underline{\alpha}) = 0 \quad \forall\, \underline{d} \in \mathbb{N}_0^n \text{ such that } \frac{d_1}{r_1} + \ldots + \frac{d_n}{r_n} < (\frac{1}{2} - 3\varepsilon)n. \quad (3.36)$$

Moreover, by elementary properties of the derivatives $\partial_{\underline{d}} Q(\underline{\alpha}) = 0$ if we have $d_j > r_j$ for some $j \in \{1, \dots, n\}$. Hence, we may assume that $d_j \leq r_j$ for all $j \in \{1, \dots, n\}$.
Again, we use the standard way of estimating $\left|\partial_{\underline{d}} Q(\underline{\alpha})\right|_{v'}$ from above, by multiplying the maximal size of a summand with the number of non-zero summands. This gives

$$\begin{aligned} \left|\partial_{\underline{d}} Q(\underline{\alpha})\right|_{v'} &\leq |Q|_{v'} \cdot \prod_{j=1}^n \binom{r_j}{d_j}^{\delta_v} \max\{1, |\alpha|_{v'}\}^{r_j - d_j} (r_j - d_j + 1)^{\delta_v} \\ &\leq |Q|_{v'} \cdot \prod_{j=1}^n 2^{\delta_v r_j} \max\{1, |\alpha|_{v'}\}^{r_j - d_j} (r_j + 1)^{\delta_v}, \end{aligned}$$

which implies

$$\begin{aligned} \log(\left|\partial_{\underline{d}} Q(\underline{\alpha})\right|_{v'}) &\leq \log(|Q|_v) + \log(\max\{1, |\alpha|_{v'}\}) \sum_{j=1}^n (r_j - d_j) + \sum_{j=1}^n \left(\log(2) + \frac{\log(r_j+1)}{r_j}\right) \delta_v r_j \\ &\overset{(3.29)}{\leq} \log(|Q|_v) + \frac{2D}{L} \log(\max\{1, |\alpha|_{v'}) \\ &\quad - \log(\max\{1, |\alpha|_{v'}) \sum_{j=1}^n d_j + \sum_{j=1}^n \left(\log(2) + \frac{\log(r_j+1)}{r_j}\right) \delta_v r_j. \end{aligned} \quad (3.37)$$

As in Lemma 2.1.25 we have for all $j \in \{1, \dots, n\}$ the estimate

$$|\alpha - \beta_j|_{v'} \leq \min\{1, |\alpha - \beta_j|_{v'}\} 2^{\delta_v} \max\{1, |\alpha|_{v'}\} \max\{1, |\beta_j|_{v'}\}.$$

This yields

$$\begin{aligned}
\left| \partial_{\underline{d}} Q(\underline{\alpha}) \prod_{j=1}^{n} (\alpha - \beta_j)^{d_j} \right|_{v'} &\leq |\partial_{\underline{d}} Q(\underline{\alpha})|_{v'} \prod_{j=1}^{n} \left(\min\{1, |\alpha - \beta_j|_{v'}\} 2^{\delta_v} \max\{1, |\alpha|_{v'}\} \max\{1, |\beta_j|_{v'}\} \right)^{d_j} \\
&\overset{d_j \leq r_j}{\leq} |\partial_{\underline{d}} Q(\underline{\alpha})|_{v'} \left(\prod_{j=1}^{n} \min\{1, |\alpha - \beta_j|_{v'}\}^{d_j} \right) 2^{\delta_v \sum_{j=1} r_j} \\
&\quad \cdot \left(\prod_{j=1}^{n} \max\{1, |\beta_j|_{v'}\}^{r_j} \right) \max\{1, |\alpha|_{v'}\}^{\sum_{j=1}^{n} d_j}.
\end{aligned}$$

Taking the logarithm, and combining this with (3.37) gives

$$\begin{aligned}
&\log\left(\left| \partial_{\underline{d}} Q(\underline{\alpha}) \prod_{j=1}^{n} (\alpha - \beta_j)^{d_j} \right|_{v'} \right) \\
\leq &\log(|Q|_v) + \frac{2D}{L} \log(\max\{1, |\alpha|_{v'}) - \log(\max\{1, |\alpha|_{v'}) \sum_{j=1}^{n} d_j \\
&+ \sum_{j=1}^{n} \left(\log(2) + \frac{\log(r_j + 1)}{r_j} \right) \delta_v r_j + \sum_{j=1}^{n} d_j \log(\min\{1, |\alpha - \beta_j|_{v'}\}) + \log(2) \delta_v \sum_{j=1}^{n} r_j \\
&+ \sum_{j=1}^{n} r_j \log(\max\{1, |\beta_j|_{v'}\}) + \log(\max\{1, |\alpha|_{v'}\}) \sum_{j=1}^{n} d_j \\
= &\log(|Q|_v) + \frac{2D}{L} \log(\max\{1, |\alpha|_{v'}\}) + \sum_{j=1}^{n} r_j \log(\max\{1, |\beta_j|_v\}) \\
&+ \sum_{j=1}^{n} \left(\log(4) + \frac{\log(r_j + 1)}{r_j} \right) \delta_v r_j + \sum_{j=1}^{n} d_j \log(\min\{1, |\alpha - \beta_j|_{v'}\}) \\
\overset{(3.29)}{\leq} &\log(|Q|_v) + \frac{2D}{L} \log(\max\{1, |\alpha|_{v'}\}) + \sum_{j=1}^{n} r_j \left(\log(\max\{1, |\beta_j|_v\}) + \frac{\log(r_j + 1)}{r_j} \delta_v \right) \\
&+ \frac{2D}{L} \log(4) \delta_v + \sum_{j=1}^{n} d_j \log(\min\{1, |\alpha - \beta_j|_{v'}\})
\end{aligned} \tag{3.38}$$

We almost got rid of the dependence on $\underline{d}$. This is good, because we want to estimate $\left| Q(\underline{\beta}) \right|_v$, and hence (keeping the Taylor expansion (3.35) in mind) we need to find the maximum of all the non-zero $\left| \partial_{\underline{d}} Q(\underline{\alpha}) \prod_{j=1}^{n} (\alpha - \beta_j)^{d_j} \right|_{v'}$. Since such a term is zero if some $d_j > r_j$, there are

at most $\prod_{j=1}^n (r_j+1)$ non zero terms. Hence, (3.38) and (3.36) imply

$$\begin{aligned}\log(\left|Q(\underline{\beta})\right|_v) &\leq \max_{\substack{\underline{d}\in\mathbb{N}_0^n \\ d_1/r_1+\ldots+d_n/r_n\geq(\frac{1}{2}-3\varepsilon)n}} \log(\left|\partial_{\underline{d}}Q(\underline{\alpha})\prod_{j=1}^n(\alpha-\beta_j)^{d_j}\right|_{v'}) + \sum_{j=1}^n \log(r_j+1)\delta_v \\ &\leq \log(|Q|_v) + \frac{2D}{L}\log(\max\{1,|\alpha|_{v'}\}) + \sum_{j=1}^n r_j\left(\log(\max\{1,|\beta_j|_v\}) + \frac{2\log(r_j+1)}{r_j}\delta_v\right) \\ &\quad + \frac{2D}{L}\log(4)\delta_v + \max_{\substack{\underline{d}\in\mathbb{N}_0^n \\ d_1/r_1+\ldots+d_n/r_n\geq(\frac{1}{2}-3\varepsilon)n}} \{\sum_{j=1}^n d_j\log(\min\{1,|\alpha-\beta_j|_{v'}\})\}\end{aligned} \tag{3.39}$$

Let us abbreviate

$$\max' = \max_{\substack{\underline{d}\in\mathbb{N}_0^n \\ d_1/r_1+\ldots+d_n/r_n\geq(\frac{1}{2}-3\varepsilon)n}} \quad \text{and} \quad \min' = \min_{\substack{\underline{d}\in\mathbb{N}_0^n \\ d_1/r_1+\ldots+d_n/r_n\geq(\frac{1}{2}-3\varepsilon)n}} .$$

Then, with (3.34) and (3.39), we conclude

$$\begin{aligned}&\sum_{v\in M_K} d_v\log(\left|Q(\underline{\beta})\right|_v) \\ &\leq \sum_{v\in M_K} d_v\log(|Q|_v) + \sum_{j=1}^n r_j\left(\sum_{v\in M_K}\left(d_v\log(\max\{1,|\beta_j|\}) + \frac{2\log(r_j+1)}{r_j}\delta_v d_v\right)\right) \\ &\quad + \sum_{v\in M_K}\delta_v d_v\frac{2D}{L}\log(4) + \sum_{v\in S}\frac{2D}{L}d_v\log(\max\{1,|\alpha|_{v'}\}) \\ &\quad + \sum_{v\in S}\max'\{\sum_{j=1}^n d_j d_v\log(\min\{1,|\alpha-\beta_j|_{v'}\})\} \\ &= dh_{\mathbb{P}}(Q) + \sum_{j=1}^n r_j d\left(h(\beta_j) + \frac{2\log(r_j+1)}{r_j}\right) + d\frac{2D}{L}\log(4) \\ &\quad + \sum_{v\in S}\frac{2D}{L}d_v\log(\max\{1,|\alpha|_{v'}\}) + \sum_{v\in S}\max'\{\sum_{j=1}^n d_j d_v\log(\min\{1,|\alpha-\beta_j|_{v'}\})\}.\end{aligned}$$

Here we have used that the sum of all $\delta_v d_v$'s is the sum of all the local degrees over ∞, which is equal to $[K:\mathbb{Q}] = d$. We know a bound for $h_{\mathbb{P}}(Q)$ from Lemma 3.5.7. Moreover, we have $r_j h(\beta_j) = \lfloor D/h(\beta_j)\rfloor\, h(\beta_j) \leq D$. We define

$$C_2 = 4C_1 + \log(16) + 2\sum_{v\in S} d_v\log(\max\{1,|\alpha|_{v'}\}),$$

which is a constant only depending on the data α, S, K. Then the last formula reads

$$\begin{aligned}\sum_{v\in M_K} d_v\log(\left|Q(\underline{\beta})\right|_v) &\leq d\cdot\left((n+\frac{C_2}{L})D + n\max_{1\leq j\leq n}\{\frac{2\log(r_j+1)}{r_j}\}\right) \\ &\quad + \sum_{v\in S}\max'\{\sum_{j=1}^n d_j d_v\log(\min\{1,|\alpha-\beta_j|_{v'}\})\}.\end{aligned} \tag{3.40}$$

All that is left to do, is to find an upper bound for

$$\sum_{v\in S} \max\nolimits' \{\sum_{j=1}^{n} d_j d_v \log(\min\{1, |\alpha-\beta_j|_{v'}\})\}.$$

Luckily, we have come across these minima before, while we were studying the approximation classes. Hence, here we need our assumption (A) that the approximations $\beta_1, \dots, \beta_j$ all lie in the same approximation class $\mathcal{C}(N, (i_v)_{v\in S})$. With this information, we get

$$\begin{aligned}
&\sum_{v\in S} \max\nolimits' \{\sum_{j=1}^{n} d_j d_v \log(\min\{1, |\alpha-\beta_j|_{v'}\})\} \overset{3.5.5}{\leq} \sum_{v\in S} \max\nolimits' \{\sum_{j=1}^{n} d_j \frac{i_v}{N} \log(\Lambda(\beta_j))\} \\
&\overset{3.26}{\leq} \sum_{v\in S} \max\nolimits' \{\sum_{j=1}^{n} d_j \frac{i_v}{N} \cdot (-\kappa d h(\beta_j))\} = -\kappa d \left(\sum_{v\in S} \frac{i_v}{N}\right) \min\nolimits' \{\sum_{j=1}^{n} d_j h(\beta_j)\} \\
&\overset{3.5.5}{\leq} -\kappa d \left(1-\frac{|S|}{N}\right) \min\nolimits' \{\sum_{j=1}^{n} d_j h(\beta_j)\}
\end{aligned}$$

As an exercise you can conclude

$$\sum_{v\in S} \max\nolimits' \{\sum_{j=1}^{n} d_j d_v \log(\min\{1, |\alpha-\beta_j|_{v'}\})\} \leq -\kappa d \left(1-\frac{|S|}{N}\right) (D-h(\beta_n))(\frac{1}{2}-3\varepsilon)n.$$

We plug this into (3.40), and use the brutal estimate $\max_{1\leq j\leq n}\{\frac{2\log(r_j+1)}{r_j}\} \leq 2\log(D)$, to finally get

$$\begin{aligned}
\sum_{v\in M_K} d_v \log(\left|Q(\underline{\beta})\right|_v) \leq d \cdot &\left((n+\frac{C_2}{L})D + n2\log(D)\right) \\
&- \kappa d \left(1-\frac{|S|}{N}\right)(D-h(\beta_n))(\frac{1}{2}-3\varepsilon)n. \qquad (3.41)
\end{aligned}$$

This obviously depends on all the chosen parameters n, L, ε, D, N, and more hidden it also depends on M. All these values have to be chosen according to (A)-(H). However, there is no further dependence on any other values not among the given data S, α, K.

3.5.4 Conclusion

For elements $n, N, M, L, \varepsilon, D$ that satisfy the conditions (A)-(H), we combine (3.41) and (3.33) to achieve

$$\kappa d \left(1-\frac{|S|}{N}\right)(D-h(\beta_n))(\frac{1}{2}-3\varepsilon)n \leq d \cdot \left((n+\frac{C_2}{L})D + n2\log(D)\right),$$

which is equivalent to

$$\kappa \left(1-\frac{|S|}{N}\right) \frac{D-h(\beta_n)}{D}(\frac{1}{2}-3\varepsilon) \leq (1+\frac{C_2}{nL}) + 2\frac{\log(D)}{D}. \qquad (3.42)$$

Now it is time to fix the parameters. Since we assume $\kappa > 2$, there is an $\varepsilon \in (0, 1/2)$, and and a positive integer N such that $\kappa(\frac{1}{2}-3\varepsilon)(1-\frac{|S|}{N}) > 1$. We fix such elements ϵ and N.

Then we fix an integer n that satisfies (D), and an M that satisfies (F). Lastly, we let D and L tend to infinity, so that the left hand side of (3.42) is greater than 1 and the right hand side is equal to 1. This is finally a contradiction, which proves that our assumption (3.26) was incorrect. This finally proves Roth's theorem 3.0.1.

Remark 3.5.8. Although it seems to be impossible to derive with these methods an effective lower bound for $\Lambda(\beta) \cdot H(\beta)^{d\kappa}$, it is possible to calculate an effective upper bound for the number of $\beta \in K$ satisfying (3.26).

Exercises

We use the notation from the previous section!

Exercise 3.8. Prove that for any $N \in \mathbb{N}$ there are strictly less than $2^{N+|S|}$ non-empty approximation classes of size $1/N$.

Exercise 3.9. Set $\alpha = \sqrt{7}$, $K = \mathbb{Q}$, and $S = \{\infty, 3\}$. Choose extensions of ∞ and 3 to $\mathbb{Q}(\alpha)$, and find $\beta_1, \beta_2, \beta_3 \in \mathbb{Q}$ such that

- $|\alpha - \beta_1|_{\infty'} < 1$, and $|\alpha - \beta_1|_{3'} \geq 1$.
- $|\alpha - \beta_1|_{\infty'} \geq 1$, and $|\alpha - \beta_1|_{3'} < 1$.
- $|\alpha - \beta_1|_{\infty'} < 1$, and $|\alpha - \beta_1|_{3'} < 1$.

Exercise 3.10. Prove the inequality

$$\min{}' \left\{ \sum_{j=1}^{n} d_j h(\beta_j) \right\} \geq (D - h(\beta_n))(\frac{1}{2} - 3\varepsilon)n.$$

Exercise 3.11. We consider the linear equations

$$\begin{aligned} L_1(\underline{x}) &= x_1 + \sqrt{2}x_2 + \sqrt{3}x_3, \\ L_2(\underline{x}) &= x_1 - \sqrt{2}x_2 + \sqrt{3}x_3, \\ L_3(\underline{x}) &= x_1 - \sqrt{2}x_2 - \sqrt{3}x_3. \end{aligned}$$

Prove that for any $\delta \in (0, 1)$ there are infinitely many triples $\underline{a} = (a_1, a_2, a_3) \in \mathbb{Z}^3$ such that

$$0 < |L_1(\underline{a}) \cdot L_2(\underline{a}) \cdot L_3(\underline{a})| \leq H(\underline{a})^{-\delta}.$$

Hint: You don't need Roth's Theorem for this exercise.

3.6 Generalizations

The version of Roth's theorem that we have just proved is already quite general compared to Roth's original result (Theorem 1.1.17). But a beautiful (and sometimes scary) property of mathematics is that you can almost always generalize further. However, we will concentrate on generalizing the concept and therefore we will stick to the setting of the usual archimedean absolute value $|.|$ on the field $\mathbb{Q}$.
The "multi-dimensional" version of Roth's theorem is Schmidt's subspace theorem, which we will not prove here.

Definition 3.6.1. Let K be any field and $n \in \mathbb{N}$. A *linear form* over K is just a homogeneous polynomial of degree 1 with coefficients in K.
A *hyperplane* in K^n is a subvector-space of K^n of dimension $n-1$.

Theorem 3.6.2. *Let $n \geq 2$ be an integer, and let $L_1, \ldots, L_n \in \overline{\mathbb{Q}}[x_1, \ldots, x_n]$ be linearly independent linear forms. For all $\varepsilon > 0$ there are finitely many hyperplanes $T_1, \ldots, T_r$ of $\mathbb{Q}^n$ such that all $\underline{p} = (p_1, \ldots, p_n) \in \mathbb{Z}^n$ with*

$$\left|L_1(\underline{p}) \cdots L_n(\underline{p})\right| < \frac{1}{\max\{|p_1|, \ldots, |p_n|\}^{\varepsilon}} \tag{3.43}$$

lie in the union $T_1 \cup \ldots \cup T_r$.

Remark 3.6.3. The statement that theses vectors $\underline{p} \in \mathbb{Z}^n$ lie in a finite number of hyperplanes means that there are very few of them. All solutions of (3.43) lie in something of dimension less then n. Hence, if $n = 2$ then all these vectors lie on a finite number of lines.
But we may wonder nevertheless whether there are indeed only finitely many vectors $\underline{p} \in \mathbb{Z}^n$ satisfying satisfying (3.43). But if there is a $\underline{p} \neq \underline{0}$ such that $L_i(\underline{p}) = 0$ for some $i \in \{1, \ldots, n\}$, then L_i vanishes for every element in $\mathbb{Z} \cdot \underline{p}$. Hence, in this case (3.43) is satisfied for the infinitely many integral vectors from $\mathbb{Z} \cdot \underline{p}$. But this is not the only obstruction! In the exercises you have shown that there is an example such that also the equation

$$0 < \left|L_1(\underline{p}) \cdots L_n(\underline{p})\right| < \frac{1}{\max\{|p_1|, \ldots, |p_n|\}^{\varepsilon}}$$

is satisfied for infinitely many $\underline{p} \in \mathbb{Z}^n$.

Remark 3.6.4. As in Remark 3.0.2, we may multiply the right hand side of (3.43) by any constant without violating the statement.

This may not look like a direct generalization of Roth's theorem. The connection becomes more obvious if we look at the following corollary.

Corollary 3.6.5. *Let $n \in \mathbb{N}$ be arbitrary and let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ such that $1, \alpha_1, \ldots, \alpha_n$ are $\mathbb{Q}$-linearly independent. Then, for every $\varepsilon > 0$ there are at most finitely many tuples $(p_1, \ldots, p_n, q) \in \mathbb{Z}^n \times \mathbb{N}$ such that*

$$\left|\alpha_i - \frac{p_i}{q}\right| < \frac{1}{q^{1+\frac{1}{n}+\varepsilon}} \quad \forall\ i \in \{1, \ldots, n\}. \tag{3.44}$$

Proof. Let $(p_1, \ldots, p_n, q) \in \mathbb{Z}^n \times \mathbb{N}$ satisfy (3.44). Then we have

$$\left(\prod_{i=1}^{n} |\alpha_i q - p_i|\right) \cdot |q| = \left(\prod_{i=1}^{n} \left|\alpha_i - \frac{p_i}{q}\right|\right) \cdot q^{n+1} < \frac{1}{q^{n\varepsilon}}. \tag{3.45}$$

Moreover, we know that for all $i \in \{1, \ldots, n\}$ we have

$$1 \geq \left|\alpha_i - \frac{p_i}{q}\right| \geq \left|\frac{p_i}{q}\right| - |\alpha_i| \quad \Longrightarrow \quad |p_i| \leq q \cdot (1 + |\alpha_i|).$$

If we define $C = \max_{1 \leq i \leq n}(1 + |\alpha_i|)$, then this implies

$$\max\{|p_1|, \ldots, |p_n|, |q|\} \leq C \cdot q \tag{3.46}$$

Combining (3.46) with (3.45) shows that we have

$$\left(\prod_{i=1}^{n} |\alpha_i q - p_i|\right) \cdot |q| < \frac{C^{n\varepsilon}}{\max\{|p_1|, \ldots, |p_n|, |q|\}^{n\varepsilon}}.$$

Hence, for all $i \in \{1, \ldots, n\}$ we define the linear forms $L_i(\underline{x}) = \alpha_i x_{n+1} - x_i \in \overline{\mathbb{Q}}[x_1, \ldots, x_{n+1}]$, and set $L_{n+1}(\underline{x}) = x_{n+1} \in \overline{\mathbb{Q}}[x_1, \ldots, x_{n+1}]$. Since any of the linear forms $L_1, \ldots, L_n$ has a variable that does not appear in the others, they are linearly independent. The linear independence of $x_1, \ldots, x_{n+1}$ then implies that also $L_1, \ldots, L_{n+1}$ are linearly independent.
Therefore, the subspace Theorem 3.6.2 (for $n\varepsilon$) implies that there are finitely many hyperplanes $T_1, \ldots, T_r \subseteq \mathbb{Q}^{n+1}$ such that $(p_1, \ldots, p_n, q) \in \mathbb{Z}^n \times \mathbb{N}$ lies in $T_1 \cup \ldots \cup T_r$. Here we have also applied Remark 3.6.4. So by now we know that there are very few tuples satisfying (3.44). We are left to prove that all of the hyperplanes $T \in \{T_1, \ldots, T_r\}$ contain at most finitely many of such tuples.
By basic linear algebra, we know that every such T is given by a single linear form; i.e. there is a linear form $L \in \mathbb{Q}[x_1, \ldots, x_{n+1}] \setminus \{0\}$ such that

$$T = \{\underline{a} \in \mathbb{Q}^{n+1} | L(\underline{a}) = 0\}$$

(just choose as a coefficient vector for L a non-zero vector in the orthogonal complement of T). We write $L(\underline{x}) = c_1 x_1 + \ldots + c_{n+1} x_{n+1}$. Then for any $(p_1, \ldots, p_n, q) \in \mathbb{Z}^n \times \mathbb{N}$, in T that satisfies (3.44), we have

$$\begin{aligned} & c_1(\alpha_1 q - p_1) + \ldots + c_n(\alpha_n q - p_n) + c_{n+1} q_{n+1} \\ =& L(q\alpha_1 - p_1, \ldots, q\alpha_n - p_n, q) \\ =& q(c_1\alpha_1 + \ldots + c_n\alpha_n + c_{n+1}) - \underbrace{(c_1 p_1 + \ldots + c_n p_n)}_{=-c_{n+1}q}. \end{aligned}$$

We subtract $c_{n+1}q$ on both sides and take the absolute value to conclude

$$q\,|c_1\alpha_1 + \ldots + c_n\alpha_n + c_{n+1} \cdot 1| = |c_1(\alpha_1 q - p_1) + \ldots + c_n(\alpha_n q - p_n)| \overset{(3.44)}{<} \left(\sum_{i=1}^{n} |c_i|\right) \cdot q^{-\frac{1}{n}-\varepsilon}.$$

But since $\alpha_1, \ldots, \alpha_n, 1$ are $\mathbb{Q}$-linearly independent and not all of the c_i's are equal to zero, we know that $|c_1\alpha_1 + \ldots + c_n\alpha_n + c_{n+1} \cdot 1| \neq 0$. Hence, q is bounded from above. But now (3.46) implies that $\max\{|p_1|, \ldots, |p_n|, q\}$ is bounded from above. This means that there are at most finitely many $(p_1, \ldots, p_n, q) \in \mathbb{Z}^n \times \mathbb{N}$ in T satisfying (3.44). This proves the corollary. □

Remark 3.6.6. The case $n = 1$ in Corollary 3.6.5 is precisely Roth's Theorem 1.1.17. This is due to the assumption that $\alpha_1, \ldots, \alpha_n, 1$ are $\mathbb{Q}$-linearly independent. This implies in particular, that non of the α_i's is a rational number. Hence, the subspace Theorem 3.6.2 is indeed a generalization of Roth's theorem.

We will not state the general subspace theorem for arbitrary number fields and a finite set of absolute values. But still we mention that such a generalized theorem does exist. As an application of this result one can prove the finiteness of the *generalized unit equation*.

Theorem 3.6.7. *Let K be a number field, and $n \in \mathbb{N}$ be arbitrary. There are at most finitely many $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K^*$ such that*

$$\alpha_1 + \ldots + \alpha_n = 1,$$

and $\sum_{i \in I} \alpha_i \neq 0$ for all non-empty subsets $I \subseteq \{1, \ldots, n\}$.

Since we have already skipped the formulation of the Subspace theorem, we skip the proof of this application as well. Note that the assumption on the non-vanishing of any subsum is necessary. Otherwise you could for instance take the infinitely many solutions $\alpha+(-\alpha)+1=1$, $\alpha \in \mathcal{O}_K^*$, for $n=3$.
As a last part in this Chapter on Roth's theorem, we will discuss the *abc*-conjecture.

Definition 3.6.8. The *radical* of an integer $n \in \mathbb{Z} \setminus \{0\}$ is the product of all different prime numbers which are divisors of n. We denote the radical of n by $\mathrm{rad}(n)$. Formally:

$$\mathrm{rad}(n) = \prod_{\substack{p|n \\ p \text{ prime}}} p.$$

***abc*-Conjecture 3.6.9.** *For all $\varepsilon > 0$ there exists a constant $C(\varepsilon)$ such that for all coprime $a, b, c \in \mathbb{N}$, with $a+b=c$, we have*

$$c \leq C(\varepsilon)\,\mathrm{rad}(abc)^{1+\varepsilon}.$$

It is tempting to fix an ε and a constant $C(\varepsilon)$, to get a special (but effective) conjecture. The following version is the most prominent.

***abc*-Conjecture 3.6.10.** *(weak version) For all coprime $a, b, c \in \mathbb{N}$ satisfying $a+b=c$ we have*

$$c \leq \mathrm{rad}(abc)^2.$$

Remark 3.6.11. In both versions of the *abc*-conjecture you may replace $a+b=c$ for natural numbers a, b, c, by $a+b+c=0$ for non-zero integers. Then the *abc*-conjecture bounds $\max\{|a|, |b|, |c|\}$ from above in terms of $\mathrm{rad}(abc)$.

Example 3.6.12. A reformulation of the weak *abc*-conjecture is, that $\log(c)/\log(\mathrm{rad}(abc)) \leq 2$. Hence, in order to search for a counterexample to the weak *abc*-conjecture, we have to find positive integers a, b, c, with $a+b=c$, such that $\log(c)/\log(\mathrm{rad}(abc))$ is large.

(a) $1+2^3=3^2$ gives $\log(c)/\log(\mathrm{rad}(abc)) = \log(9)/\log(6)$.

(b) $2+3^{10}\cdot 109 = 23^5$ gives $\log(c)/\log(\mathrm{rad}(abc)) = 5\log(23)/\log(2\cdot 3\cdot 109\cdot 23) = 1,6299...$ This is the currently largest known value for $\log(c)/\log(\mathrm{rad}(abc))$. It was constructed by Eric Reyssat.

Let us shortly give the idea how to construct examples of triples with $\log(c)/\log(\mathrm{rad}(abc)) \geq 1$: If we take a positive integer A and a convergent $\frac{p_n}{q_n}$ of $\sqrt[k]{A}$. Then

$$\sqrt[k]{A} = \frac{p_n}{q_n} + (\text{error term of absolute value } < \frac{1}{q_n q_{n+1}}).$$

But this means that $q_n^k A - p_n^k$ is roughly of size p_n^{k-1}/q_{n+1}, which is small compared with p_n^k and q_n^k. This is, using $a, b, c \in \mathbb{N}$ among $\pm(q_n^k A - p_n^k)$, $\pm p_n^k$, and $\pm q_n^k A$ to satisfy $a+b=c$, we expect

$$\log(c)/\log(\mathrm{rad}(abc)) > \log(q_n^k A)/\log(p_n q_n A p_n^{k-1}/q_{n+1}) > 1.$$

Moreover, if p_n, q_n or $q_n^k A - p_n^k$ has any prime power factors or q_{n+1} is large, we expect that the left hand side is much larger than the right hand side. To give things names, we note that $\sqrt[5]{109} = \langle 2, 1, 1, 4, 77733, \ldots\rangle$. The third convergent of $\sqrt[5]{109}$ is $\frac{23}{9}$. Hence, 23^5, $9^5 109$, and $-(23^5 - 9^5 109) = 2$ gives the example above. This example is that good, since we have the huge term 77733, and 9 is a prime power.

Remark 3.6.13. This is a very popular conjecture in number theory. It was in the news for quite some time since a very well established mathematician, Shinichi Mochizuki, claims since 2012 to have found a proof of (a generalized version of) the *abc* conjecture. His work contains roughly 500 pages, and most mathematicians do not understand too much of what is going on there. However, in 2018 Peter Scholze and Jakob Stix (also most respected mathematicians) reported to have found a fundamental error in Mochizuki's proof. They give an precise explanation on where this error occurs. It exists a written answer to this by Mochizuki, which unfortunately does not shed any light on the issue. I will deliberately not take any position concerning the correctness of the proof. But what I can certainly claim, and give you as an advice: A mathematical proof is worthless, if it is not written in a way that experts in the field can understand it. (In your case you should replace "experts in the field" by "your lecturer".)
However! Why on earth does this number theoretical conjecture appear in a chapter on Roth's theorem? The answer is the following rule of thumb:

$$abc \quad \Longrightarrow \quad \text{everything}$$

Example 3.6.14. The weak *abc*-conjecture 3.6.10 implies Fermat's last theorem; i.e. for any integer $n \geq 3$ there are no integral solutions $(a, b, c) \in \mathbb{N}^3$ to the equation $x^n + y^n = z^n$.
Assume there are $a, b, c \in \mathbb{N}$ such that $a^n + b^n = c^n$. Then the weak *abc*-conjecture tells us

$$c^n < \mathrm{rad}(a^n b^n c^n)^2 \leq (abc)^2 < c^{3\cdot 2}.$$

Hence, we must have $n < 6$. Now the statement follows from the fact that Fermat's last theorem for $n = 3$, $n = 4$, and $n = 5$ is well known. The cases are due to Euler, Fermat, and Dirichlet and Legendre.

You can guess what we are going to prove next:

Theorem 3.6.15. *The abc-Conjecture 3.6.9 implies Roth's Theorem 1.1.17.*

To prove this we need some results concerning ramified morphisms. Some of you have already visited courses on algebraic geometry, others not. Hence, we will only recall the basic definitions in the special setting we are going to use. The results from algebraic geometry will be used as a black box.

Definition 3.6.16. Let F be a subfield of $\mathbb{C}$. A *morphism* of degree d from $\mathbb{P}^N(\mathbb{C}) \longrightarrow \mathbb{P}^M(\mathbb{C})$ is given by homogeneous polynomials $f_0, \ldots, f_M \in F[x_0, \ldots, x_N]$ of degree d, such that $f_0, \ldots, f_M$ have no non-trivial common root. The morphism is *defined over* F, if the polynomials $f_0, \ldots, f_M$ can be chosen from $F[x_0, \ldots, x_N]$.

Remark 3.6.17. Let F be subfield of $\mathbb{C}$. If $[a : b] \in \mathbb{P}^1(F)$ with $b \neq 0$, then we have $[a : b] = [a/b : 1]$. Hence, we can regard $\mathbb{P}^1(F)$ as the set $F \cup \{\infty\}$, by identifying $[a : b]$ with a/b if $b \neq 0$, and $[1 : 0](= [a : 0])$ for all $a \neq 0$) with ∞.
Then any rational function $u(x)/v(x) \in F(x)$ of degree d can uniquely be identified with a morphism from $\mathbb{P}^1$ to $\mathbb{P}^1$. We first cancel out common factors, so that u and v are coprime and $d = \max\{\deg(u), \deg(v)\}$. This implies that $U(X, Y) = Y^d u(X/Y)$ and $V(X, Y) = Y^d v(X/Y)$ are homogeneous polynomials of degree d without a non-trivial root. Hence the

map $\varphi([a:b]) = [U(a,b) : V(a,b)]$ is a morphism. Moreover, we have for all $a, b \in \overline{\mathbb{Q}}$ with $b \neq 0$

$$\varphi([a:b]) = [U(a,b) : V(a,b)] \hat{=} \begin{cases} \frac{u(a/b)}{v(a/b)} & \text{if } v(a/b) \neq 0 \\ \infty & \text{if } v(a/b) = 0. \end{cases}$$

Hence, this morphism is compatible with our identification of $\mathbb{P}^1(F)$ with $F \cup \{\infty\}$ and extends the rational function $u(x)/v(x)$ to the point at infinity.
This transformation works in both directions. This is, given any morphism $[U(X,Y) : V(X,Y)]$ defined over F, there are $u, v \in F(x)$ such that the morphism coincides with the map $u(x)/v(x)$. In particular, when working with a morphism on $\mathbb{P}^1$ to $\mathbb{P}^1$ at a point different from $[1:0]$, we can safely regard the morphism as a well known rational function in a single variable. Using this conceptions, it is clear that the composition $\varphi \circ \Psi$ of two morphisms $\varphi, \Psi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ is again a morphism.

In the exercises we have already come across the generalization of Theorem 3.1.1, which we recall here:

Theorem 3.6.18. *Let $\varphi : \mathbb{P}^N(\overline{\mathbb{Q}}) \longrightarrow \mathbb{P}^M(\overline{\mathbb{Q}})$ be a morphism of degree d. Then there is a constant c_φ only depending on φ such that for all $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$ we have*

$$c_\varphi^{-1} H(P)^d \leq H(\varphi(P)) \leq c_\varphi H(P)^d.$$

Definition 3.6.19. A morphism $\varphi : \mathbb{P}^1(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C})$ of degree d is *ramified at a point* $P \in \mathbb{P}^1(\mathbb{C})$, if $\big|\{Q \in \mathbb{P}^1(\mathbb{C}) | \varphi(Q) = P\}\big| < d$. Consequently, φ is *unramified at a point* P, if $\big|\{Q \in \mathbb{P}^1(\mathbb{C}) | \varphi(Q) = P\}\big| = d$.

Note that by the preceding remark and the fundamental theorem of Algebra it is obvious that for all $P \in \mathbb{P}^1(\mathbb{C})$ we have $\big|\{Q \in \mathbb{P}^1(\mathbb{C}) | \varphi(Q) = P\}\big| \leq d$. Moreover, one can prove that there are at most finitely many points in $\mathbb{P}^1(\mathbb{C})$ at which φ is ramified.

Lemma 3.6.20. *Let $\varphi : \mathbb{P}^1(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C})$ be a morphism of degree d defined over $\mathbb{Q}$ given by $[X:Y] \mapsto [U(X,Y) : V(X,Y)]$. We set $W(X,Y) = V(X,Y) - U(X,Y)$, and factor U, V, W over $\mathbb{Q}[X,Y]$ into*

$$\begin{aligned} U(X,Y) &= U_1(X,Y)^{a_1} \cdots U_r(X,Y)^{a_r} \\ V(X,Y) &= V_1(X,Y)^{b_1} \cdots V_s(X,Y)^{b_s} \\ W(X,Y) &= W_1(X,Y)^{c_1} \cdots W_t(X,Y)^{c_t}, \end{aligned}$$

where the factors $U_1, \ldots, U_r$ are irreducible in $\mathbb{Q}[X,Y]$ and pairwise distinct, and so are the $V_1, \ldots, V_s$ and the $W_1, \ldots, W_t$. Then

(i) the factors $U_1, \ldots, U_r, V_1, \ldots, V_s, W_1, \ldots, W_t$ are pairwise distinct,

(ii) $\big|\{Q \in \mathbb{P}^1(\mathbb{C}) | \varphi(Q) = [0:1]\}\big| = \sum_{i=1}^r \deg(U_i)$,

(iii) $\big|\{Q \in \mathbb{P}^1(\mathbb{C}) | \varphi(Q) = [1:0]\}\big| = \sum_{i=1}^s \deg(V_i)$, and

(iv) $\big|\{Q \in \mathbb{P}^1(\mathbb{C}) | \varphi(Q) = [1:1]\}\big| = \sum_{i=1}^t \deg(W_i)$.

Proof. U and V have no common factor by the definition of a morphism. Since $W = V - U$, also W and V, resp. W and U cannot have a common factor. This proves part (i). For the other parts, we only have to note that

- $\varphi([a:b]) = [0:1]$ if and only if $U(a,b) = 0$,
- $\varphi([a:b]) = [1:0]$ if and only if $V(a,b) = 0$,
- $\varphi([a:b]) = [1:1]$ if and only if $W(a,b) = V(a,b) - U(a,b) = 0$.

Since any irreducible binary form (homogeneous polynomial in two variables)of degree k has precisely k different roots in $\mathbb{P}^1(\mathbb{C})$, the lemma is proved. □

Now we present two results for which we need all of this.

Theorem 3.6.21 (weak Riemann-Hurwitz Formula)**.** *Let $\varphi : \mathbb{P}^1(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C})$ be a morphism of degree d. Then we have*

$$2d - 2 = \sum_{P \in \mathbb{P}^1(\mathbb{C})} \left(d - \left| \{ Q \in \mathbb{P}^1(\mathbb{C}) | \varphi(Q) = P \} \right| \right).$$

The proof should be part of any algebraic geometry course. Otherwise, you can find this special version in [12].

Lemma 3.6.22 (Belyi's Lemma)**.** *Let $\varphi : \mathbb{P}^1(\overline{\mathbb{Q}}) \longrightarrow \mathbb{P}^1(\overline{\mathbb{Q}})$ be a morphism of degree $d \geq 1$ defined over a number field K, and let $S \subseteq \mathbb{P}^1(\overline{\mathbb{Q}})$ be finite. There exists a morphism $\Psi : \mathbb{P}^1(\overline{\mathbb{Q}}) \longrightarrow \mathbb{P}^1(\overline{\mathbb{Q}})$ defined over K such that the morphism $\Psi \circ \varphi : \mathbb{P}^1(\overline{\mathbb{Q}}) \longrightarrow \mathbb{P}^1(\overline{\mathbb{Q}})$ satisfies*

(i) $\Psi \circ \varphi$ is unramified outside $\{[0:1], [1:1], [1:0]\}$, and

(ii) $\Psi \circ \varphi(S) \subseteq \{[0:1], [1:1], [1:0]\}$.

Note that the set $\{[0:1], [1:1], [1:0]\}$ is the same as $\{0, 1, \infty\}$ if we use rational functions in $\overline{\mathbb{Q}}(x)$. The proof of this result can be found in [1], Lemma 12.2.7.
With these two black-boxes we can prove that the *abc*-conjecture 3.6.9 implies Roth's Theorem 1.1.17.

Proof of Theorem 3.6.15. We fix an algebraic number α of degree $d \geq 2$ and an $\varepsilon > 0$. Moreover we assume $\varepsilon < d$ which is of course no restriction at all. We have to prove that there is a constant $c(\alpha, \varepsilon)$ such that $\left| \alpha - \frac{p}{q} \right| \geq \frac{c(\alpha,\varepsilon)}{|q|^{2+\varepsilon}}$ for all coprime $p, q \in \mathbb{Z}$.
We denote the minimal polynomial of α over $\mathbb{Z}$ by $f(x)$. This polynomial is in particular a morphism from $\mathbb{P}^1(\overline{\mathbb{Q}})$ to $\mathbb{P}^1(\overline{\mathbb{Q}})$, defined by $[a:b] \mapsto [F(X,Y) : Y^d]$, with $F(X,Y) = Y^d f(X/Y)$. Let $S \subseteq \mathbb{P}^1(\overline{\mathbb{Q}})$ be the finite set of roots of $f(x)$. By Belyi's Lemma 3.6.22 there is a morphism $\Psi : \mathbb{P}^1(\overline{\mathbb{Q}}) \longrightarrow \mathbb{P}^1(\overline{\mathbb{Q}})$, such that $\varphi = \Psi \circ f$ is defined over $\mathbb{Q}$, and

(i) φ is unramified outside $\{[0:1], [1:1], [1:0]\}$, and

(ii) $\varphi(S) = \Psi(f(S)) = \Psi([0:1]) \in \{[0:1], [1:1], [1:0]\}$.

Let τ be any of the morphisms $[a:b] \mapsto [b:a]$ or $[a:b] \mapsto [b-a:b]$. Then $\tau \circ \tau$ is the identity map. Hence, for all $P \in \mathbb{P}^1(\overline{\mathbb{Q}})$ we have

$$\left| \{ Q \in \mathbb{P}^1(\overline{\mathbb{Q}}) | \tau \circ \varphi(Q) = P \} \right| = \left| \{ Q \in \mathbb{P}^1(\overline{\mathbb{Q}}) | \varphi(Q) = \tau(P) \} \right|.$$

Since we have also

$$\tau(P) \in \{[0:1], [1:1], [1:0]\} \quad \Longleftrightarrow \quad P \in \{[0:1], [1:1], [1:0]\},$$

we may replace Ψ by $\tau \circ \Psi$ without violating assumptions (i) and (ii). Hence, we may assume that

$$\Psi([0:1]) = [0:1]. \tag{3.47}$$

Let $n \geq d$ be the degree of φ, and let $U(X,Y), V(X,Y) \in \mathbb{Z}[X,Y]$ be homogeneous polynomials of degree n such that φ is given by $[a:b] \mapsto [U(a,b) : V(a,b)]$. Moreover, we define $W(X,Y) = V(X,Y) - U(X,Y) \in \mathbb{Z}[X,Y]$, which is still homogeneous of degree n. The associated "dehomogenized" polynomials in one variable, are $u, v, w \in \mathbb{Z}[x]$ such that

$$u(X/Y) = \frac{1}{Y^n}U(X,Y), \quad v(X/Y) = \frac{1}{Y^n}V(X,Y), \quad w(X/Y) = \frac{1}{Y^n}W(X,Y).$$

Since α is a root of f, we have $\varphi([\alpha:1]) \overset{(ii)}{=} \Psi([0:1]) = [0:1]$. Moreover, $u(x)$ and $v(x)$ have no common factor in $\mathbb{C}[x]$. We conclude

$$u(\alpha) = 0, \quad v(\alpha) \neq 0, \quad w(\alpha) = v(\alpha) - u(\alpha) \neq 0. \tag{3.48}$$

As in Lemma 3.6.20 we factor

$$\begin{aligned} U(X,Y) &= u_0 U_1(X,Y)^{a_1} \cdots U_r(X,Y)^{a_r} \\ V(X,Y) &= v_0 V_1(X,Y)^{b_1} \cdots V_s(X,Y)^{b_s} \\ W(X,Y) &= w_0 W_1(X,Y)^{c_1} \cdots W_t(X,Y)^{c_t}, \end{aligned}$$

with $U_i(X,Y), V_i(X,Y), W_i(X,Y) \in \mathbb{Z}[X,Y]$ irreducible, and $u_0, v_0, w_0 \in \mathbb{Z}$. Since φ is unramified outside of $\{[0:1],[1:1],[1:0]\}$, the Riemann-Hurwitz Formula 3.6.21 tells us

$$\begin{aligned} 2n-2 &= \sum_{P \in \{[0:1],[1:1],[1:0]\}} \left(n - \left|\{Q \in \mathbb{P}^1(\mathbb{C}) | \varphi(Q) = P\}\right|\right) \\ &\overset{3.6.20}{=} \left(n - \sum_{i=1}^{r} \deg(U_i)\right) + \left(n - \sum_{i=1}^{s} \deg(V_i)\right) + \left(n - \sum_{i=1}^{t} \deg(W_i)\right). \end{aligned}$$

Thus,

$$n + 2 = \sum_{i=1}^{r} \deg(U_i) + \sum_{i=1}^{s} \deg(V_i) + \sum_{i=1}^{t} \deg(W_i). \tag{3.49}$$

By (3.48) we have $U(\alpha, 1) = u(\alpha) = 0$. In particular, since $F(X,Y) = Y^d f(X/Y) \in \mathbb{Z}[X,Y]$ is irreducible (recall that f is the minimal polynomial of α), we may assume

$$U_1(X,Y) = Y^d f(X/Y).$$

Now, where the black-boxes have been applied, we can start with the construction of the lower bound for rational approximations of α. Since Roth's theorem is trivial for $\alpha \notin \mathbb{R}$ we may assume $\alpha \in \mathbb{R}$. Hence, let $p, q \in \mathbb{Z}$ be coprime, and consider the approximation $\left|\alpha - \frac{p}{q}\right|$, which we want to bound from below. To this end, we may assume right from the start that $p, q \in \mathbb{Z}$ are chosen such that $\left|\alpha - \frac{p}{q}\right|$ is small. More precisely, we will assume that $\left|\alpha - \frac{p}{q}\right|$ is small enough to satisfy

(A) $\left|\alpha - \frac{p}{q}\right| < 1$, which implies $|p| \leq \underbrace{(1 + |\alpha|)}_{=c_0(\alpha)} |q|$ (see (3.46)).

(B) $|v(p/q)| \geq c_1(\alpha) > 0$, which is possible since $v(\alpha) \neq 0$ by (3.48).

(C) $|f'(\zeta)| > 0$ for all $\zeta \in \mathbb{R}$ with $|\alpha - \zeta| \leq \left|\alpha - \frac{p}{q}\right|$, which is possible since $f'(\alpha) \neq 0$.

(D) $U(p,q)V(p,q)W(p,q) \neq 0$, which is possible since uvw only have finitely many roots.

These $c_0(\alpha), c_1(\alpha)$ are constants only depending on α. There will come some more of these constants, all denoted by $c_i(\alpha)$. For instance we define $c_2(\alpha) = \max_{|\alpha-\zeta|<1} |f'(\zeta)|$. By the mean value theorem, we have $|f(p/q)| = |f(p/q) - f(\alpha)| = \left|\alpha - \frac{p}{q}\right| \cdot |f'(\zeta)|$ for some $\zeta \in \mathbb{R}$ such that $|\zeta - \alpha| \leq \left|\alpha - \frac{p}{q}\right| \overset{(A)}{\leq} 1$. Hence, by assumption (C) we can conclude that

$$c_2(\alpha)\left|\alpha - \frac{p}{q}\right| \geq f(\frac{p}{q}).^1 \tag{3.50}$$

Hence, we have to bound $f(p/q)$ from below. We will come back to this observation at the end of the proof.
Since $U(X,Y), V(X,Y), W(X,Y)$ have no common factor (see Lemma 3.6.20), we have a morphism

$$\Phi : \mathbb{P}^1(\overline{\mathbb{Q}}) \longrightarrow \mathbb{P}^2(\overline{\mathbb{Q}}) \quad ; \quad [a:b] \mapsto [U(a,b) : V(a,b) : W(a,b)]$$

of degree n defined over $\mathbb{Q}$. By Theorem 3.6.18 there is a constant $c_4(\alpha) > 0$ only depending on Φ (and Φ only depends on φ, and φ only depends on Ψ and f, and Ψ only depends on f, and f only depends on α) such that

$$H([p:q])^n \leq c_4(\alpha) H(\Phi([p:q])) = c_4(\alpha) H([U(p,q) : V(p,q) : W(p,q)]).$$

Since p, q are coprime and $U(p,q), V(p,q), W(p,q) \in \mathbb{Z}$, this is nothing but

$$\max\{|p|, |q|\}^n \leq c_4(\alpha) \frac{\max\{|U(p,q)|, |V(p,q)|, |W(p,q)|\}}{\gcd(U(p,q), V(p,q), W(p,q))}.$$

The usual estimate

$$|U(p,q)| \leq (\text{maximal coefficient of } U) \cdot \underbrace{(\text{number of non-zero coefficients of } U)}_{\leq n+1} \cdot \max\{|p|, |q|\}^n \tag{3.51}$$

(and for V and W as well) yield that there is some constant $c_5(\alpha) > 0$ only depending on α such that

$$\max\{|p|, |q|\}^n \leq c_5(\alpha) \frac{\max\{|p|, |q|\}^n}{\gcd(U(p,q), V(p,q), W(p,q))},$$

and hence

$$\gcd(U(p,q), V(p,q), W(p,q)) \leq c_5(\alpha). \tag{3.52}$$

We set

$$a = \frac{U(p,q)}{\gcd(U(p,q), V(p,q), W(p,q))}$$
$$b = -\frac{V(p,q)}{\gcd(U(p,q), V(p,q), W(p,q))}$$
$$c = \frac{W(p,q)}{\gcd(U(p,q), V(p,q), W(p,q))}.$$

[1] Note that this inequality leads to Liouville's theorem 1.1.12.

These are coprime non-zero (see (D)) integers satisfying $a+b+c=0$. We can apply the bound (3.51) for every factor U_i, V_i, W_i to conclude

$$|U_i(p,q)| \leq c_6(\alpha)\max\{|p|,|q|\}^{\deg(U_i)} \overset{(A)}{\leq} c_6(\alpha)c_0(\alpha)^{\deg(U_i)}|q|^{\deg(U_i)} \overset{(3.49)}{\leq} c_6(\alpha)c_0(\alpha)^{n+2}|q|^{\deg(U_i)}$$

(and the same holds for V_i and W_i). Since taking the radical of an integer means to erase all exponents from the prime-factorization, we know that

$$\begin{aligned}\operatorname{rad}(abc) &\leq \left| u_0v_0w_0 \underbrace{U_1(p,q)}_{=F(p,q)} \cdots U_r(p,q)\cdot V_1(p,q)\cdots V_s(p,q)\cdot W_1(p,q)\cdots W_t(p,q)\right| \\ &\leq |F(p,q)|\cdot c_7(\alpha)\,|q|^{-\deg(F)+\sum_{i=1}^r \deg(U_i)+\sum_{i=1}^s\deg(V_i)+\sum_{i=1}^t\deg(W_i)} \\ &\overset{(3.49)}{=} c_7(\alpha)\,|F(p,q)|\,|q|^{-d+2+n}\,. \end{aligned} \tag{3.53}$$

Now it is finally time to apply the *abc*-conjecture 3.6.9 for $\varepsilon' = \frac{\varepsilon}{n-\varepsilon} > 0$. This tells us, that there is a constant $C(\varepsilon')>0$ such that

$$\max\{|a|,|b|,|c|\} \leq C(\varepsilon)\operatorname{rad}(abc)^{1+\varepsilon'} \overset{(3.53)}{\leq} C(\varepsilon)c_7(\alpha)^{1+\varepsilon'}|F(p,q)|^{1+\varepsilon'}|q|^{(-d+2+n)(1+\varepsilon')}\,.$$

But we already know that

$$\begin{aligned}|b| &= \left|\frac{V(p,q)}{\gcd(U(p,q),V(p,q),W(p,q))}\right| \overset{(3.52)}{\geq} c_5(\alpha)^{-1}|V(p,q)| = c_5(\alpha)^{-1}|q|^n\,|v(p/q)| \\ &\overset{(B)}{\geq} c_5(\alpha)^{-1}c_1(\alpha)\,|q|^n\,.\end{aligned}$$

Hence, plugging this into the last displayed formula and combine all constants, gives

$$\begin{aligned} & |q|^n \leq C_0(\varepsilon,\alpha)\,|F(p,q)|^{1+\varepsilon'}\,|q|^{(-d+2+n)(1+\varepsilon')} \\ \Longrightarrow\quad & |q|^d\,|f(p/q)| = |F(p,q)| \geq C_1(\varepsilon,\alpha)\,|q|^{d-2-n\frac{\varepsilon'}{1+\varepsilon'}} = C_1(\varepsilon,\alpha)\,|q|^{d-2-\varepsilon} \\ \overset{(3.50)}{\Longrightarrow}\quad & |q|^d\,c_2(\alpha)\left|\alpha-\frac{p}{q}\right| \geq C_1(\varepsilon,\alpha)\,|q|^{d-2-\varepsilon} \\ \Longrightarrow\quad & c_2(\alpha)\left|\alpha-\frac{p}{q}\right| \geq C_1(\varepsilon,\alpha)\,|q|^{-2-\varepsilon}\,. \end{aligned} \tag{3.54}$$

for some constant $C_1(\varepsilon,\alpha)>0$ only depending on α and ε. Noting that $c_2(\alpha)^{-1}C_1(\alpha,\varepsilon)$ is still a positive constant only depending on α and ε, proves Roth's Theorem 1.1.17. □

Remark 3.6.23. In the proof we tried to keep track of how to build the final constant. All these constants are perfectly effective, once you know that the map Ψ can be constructed effectively. This is, if one would know the constant $C(\varepsilon)$ in the *abc*-conjecture for all $\varepsilon>0$, then one gets an effective bound in Roth's theorem!

We conclude by stating an *abc*-conjecture for arbitrary number fields.

abc-**Conjecture 3.6.24** (for number fields)**.** *Let K be a number field, and chose for every $v \in M_K^{\mathrm{fin}}$ an uniformizer π_v. For every $\varepsilon \in (0,1)$ there exists a constant $c_K(\varepsilon)$ such that for every $\alpha \in K \setminus \{0,1\}$ we have*

$$(1-\varepsilon)[K:\mathbb{Q}]h(\alpha) \leq \sum_{\substack{|\alpha|_v<1 \\ v\in M_K^{\mathrm{fin}}}} \log|1/\pi_v|_v^{d_v} + \sum_{\substack{|1-\alpha|_v<1 \\ v\in M_K^{\mathrm{fin}}}} \log|1/\pi_v|_v^{d_v} + \sum_{\substack{|1/\alpha|_v<1 \\ v\in M_K^{\mathrm{fin}}}} \log|1/\pi_v|_v^{d_v} + c_K(\varepsilon).$$

This is unfortunately not as neat as the *abc*-conjecture over $\mathbb{Q}$ (in the exercises you will show that for $K=\mathbb{Q}$, both *abc*-conjectures coincide). The statement is incredibly strong. It not only implies the general form of Roth's theorem 3.0.1 we have proved in the last section, it also implies a far reaching generalization of the subspace theorem 3.6.2 (and much more, but let us focus on applications to Diophantine Approximation).

Exercises

Exercise 3.12. Prove that the subspace theorem implies the following: Let $\alpha_1,\ldots,\alpha_{n+1} \in \overline{\mathbb{Q}}$ be arbitrary. Then for any $\varepsilon > 0$ there are at most finitely many $\underline{p} = (p_1,\ldots,p_{n+1}) \in \mathbb{Z}^{n+1}$ such that

$$0 < |\alpha_1 p_1 + \ldots + \alpha_{n+1}p_{n+1}| \leq H(\underline{p})^{-n-\varepsilon}.$$

Exercise 3.13. Show that the *abc*-conjecture for number fields 3.6.24, with $K=\mathbb{Q}$, is equivalent to the *abc*-conjecture 3.6.9.

Exercise 3.14. We know that 2^3 and 3^2 are successive integers. The Catalan conjecture, proved in 2002 by Preda Mihailescu, predicts that no other perfect powers of two integers can differ only by 1. This is, for any $m,n \geq 2$ the equation $x^m+1=y^n$ has no integral solution with $|x|,|y| \geq 2$ if $(m,n) \neq (3,2)$. If $(m,n)=(3,2)$, then the only integral solutions with $|x|,|y| \geq 2$ are $x=2, y=\pm 3$. Prove that the weak *abc*-conjecture implies Catalan's conjecture.
Hint: You may use that Catalan's conjecture is known in the following cases:

- $m=2$,
- $n=2$,
- $(m,n) \in \{(3,5),(5,3)\}$.

Exercise 3.15. Prove that the *abc*-conjecture is false for $\varepsilon = 0$.
Hint: You could play around a bit with $3^{2^n}-1$.

Chapter 4

Linear Forms in Logarithms

This chapter can only serve as an outlook on another important topic in Diophantine Approximations. As the name suggests, we want to study "the" logarithm function. However, our (at least my) favourite objects are algebraic numbers. Hence, we want to study $\log(\alpha)$ for an arbitrary $\alpha \in \overline{\mathbb{Q}} \subseteq \mathbb{C}$. However, there is no unique logarithm on $\mathbb{C}$. I will briefly describe what we mean by $\log(z)$ for a $z \in \mathbb{C}^*$. If for some reason this is new for you, please take your favourite book on complex analysis and learn things properly.
The usual exponential map $x \mapsto e^x$ for all $x \in \mathbb{R}$ has a unique analytic continuation to $\mathbb{C}$. Hence, the map $z \mapsto e^z$ is an entire function on $\mathbb{C}$. It is defined by the usual power series:

$$e^z = \sum_{n \geq 0} \frac{z^n}{n!} \quad \forall\, z \in \mathbb{C}.$$

You should know the beautiful Euler's formula $e^{i\pi} + 1 = 0$. More generally, for any $z \in \mathbb{C}$ we have $e^{iz} = \cos(z) + i\sin(z)$ (just compare the potential series of cos and sin with the definition of e^z). A logarithm should be an inverse of this exponential function. So, writing a non-zero complex number in polar coordinates $z = |z|\, e^{i\theta}$ for some $\theta \in \mathbb{R}$, which indicates the angle of z with the positive real axes, we want to have $\log(z) = \log(|z|\, e^{i\theta}) = \log(|z|) + i\theta$. Unfortunately, this θ is not uniquely determined, since we have $e^{i\theta} = e^{i(\theta+2\pi)}$ (rotating an angle by 2π further, does not change anything). Hence $\log(z) = \log(|z|) + i(\theta + 2\pi)$ is an equally good choice for the logarithm of z. The same is true for $\log(z) = \log(|z|) + i(\theta + 2k\pi)$ for all $k \in \mathbb{Z}$. Hence, the inverse of the exponential map is multi-valued.
For the rest of this chapter we fix any real semi-open interval I of length 2π, and assume that $\log(z)$ has imaginary part in I for all $z \in \mathbb{C}^*$. (This is, we fix one branch of this multi-valued function.) The results are independent on this choice of I, but nevertheless you should keep in mind that some choice is involved. In particular, for $z, w \in \mathbb{C}$, with $z \neq 0$, we set

$$z^w = e^{\log(z) \cdot w}$$

for our choice of the logarithm.

4.1 The Gelfond-Schneider Theorem

We have started this lecture with some results on transcendence theory, and we aim to finish it by such results. Maybe the most prominent example is the following.

Theorem 4.1.1 (Lindemann-Weierstraß)**.** *Let $\alpha_1, \dots, \alpha_n \in \overline{\mathbb{Q}}$ be pairwise distinct, then the elements $e^{\alpha_1}, \dots, e^{\alpha_n}$ are $\overline{\mathbb{Q}}$-linearly independent.*

We will not present the proof of the theorem.

Example 4.1.2. We will give the main examples of transcendental numbers:

(i) For any $\alpha \in \overline{\mathbb{Q}}^*$ the number e^α is transcendental. Simply chose $\alpha_1 = 0$ and $\alpha_2 = \alpha$. Then the Lindemann-Weierstraß theorem gives that 1 and e^α are $\overline{\mathbb{Q}}$-linearly independent. In particular, e^α is not in $\overline{\mathbb{Q}}$ since otherwise $e^\alpha \cdot 1 - 1 \cdot e^\alpha = 0$ would give a contradiction.

(ii) π is transcendental, since otherwise $i \cdot \pi$ would be in $\overline{\mathbb{Q}}^*$, and hence 1 and $e^{i\pi} = -1$ would be $\overline{\mathbb{Q}}$-linearly independent.

(iii) The same argument as in (ii) proves that $\log(\alpha)$ is transcendental for all $\alpha \in \overline{\mathbb{Q}}^* \setminus \{1\}$.

(iv) If $\alpha \in \overline{\mathbb{Q}}^*$, then $\sin(\alpha)$ and $\cos(\alpha)$ are transcendental. Let $\alpha \in \overline{\mathbb{Q}}^*$ be arbitrary. Then we set $\alpha_1 = 0$, $\alpha_2 = i\alpha$, $\alpha_3 = -i\alpha$, and conclude that $e^{i\alpha} = \cos(\alpha) + i \cdot \sin(\alpha)$, $e^{-i\alpha} = \cos(\alpha) - i \cdot \sin(\alpha)$, 1 are $\overline{\mathbb{Q}}$-linearly independent. Hence $\cos(\alpha) \notin \overline{\mathbb{Q}}$ since otherwise we had the contradictory statement

$$1 \cdot e^{i\alpha} + 1 \cdot e^{-i\alpha} - 2\cos(\alpha) \cdot e^0 = 0.$$

The fact that $\sin(\alpha)$ is transcendental follows in the same way.

Since we still want to prove something, let us prove the next big theorem in transcendental number theory.

Theorem 4.1.3 (Gelfond-Schneider)**.** *Let $\alpha, \beta \in \overline{\mathbb{Q}}$ such that $\alpha \notin \{0, 1\}$ and $\beta \notin \mathbb{Q}$. Then α^β is transcendental.*

Keep in mind, that α^β depends on a choice of the logarithm of α. The validity of the statement, however, does not depend on this choice.
Now you can construct an arbitrary number of transcendental numbers. For instance Gelfond-Schneider constant $2^{\sqrt{2}}$ is transcendental, and so is the Gelfond constant $e^\pi = (-1)^{-i}$. Before we start with the proof, we give two corollaries (actually the second is just a rewording of the first one).

Corollary 4.1.4. *Let $\alpha, \beta \in \overline{\mathbb{Q}}^*$, with $\alpha \neq 1$, then either $\frac{\log(\beta)}{\log(\alpha)} \in \mathbb{Q}$ or $\frac{\log(\beta)}{\log(\alpha)}$ is transcendental.*

Proof. Assume that there are $\alpha, \beta \in \overline{\mathbb{Q}}^*$, with $\alpha \neq 1$, such that $\frac{\log(\beta)}{\log(\alpha)} \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$. Then the Gelfond-Schneider theorem 4.1.3 states that

$$\alpha^{\frac{\log(\beta)}{\log(\alpha)}} = \left(e^{\log(\alpha)}\right)^{\frac{\log(\beta)}{\log(\alpha)}} = e^{\log(\beta)} = \beta$$

is transcendental, which is nonsense. This contradiction proves the corollary. □

Corollary 4.1.5. *Let $\alpha, \beta \in \overline{\mathbb{Q}}^*$. If $\log(\alpha)$ and $\log(\beta)$ are $\mathbb{Q}$-linearly independent, and $\gamma_1, \gamma_2 \in \overline{\mathbb{Q}}$ not both equal to zero, then*

$$\gamma_1 \log(\alpha) + \gamma_2 \log(\beta) \neq 0.$$

Proof. Since $\log(\alpha)$, $\log(\beta)$ are $\mathbb{Q}$-linearly independent, we have $\log(\alpha) \neq 0 \neq \log(\beta)$, and $\frac{\log(\beta)}{\log(\alpha)} \notin \mathbb{Q}$. Hence, if $\gamma_1 \log(\alpha) + \gamma_2 \log(\beta) = 0$ for some $\gamma_1, \gamma_2 \in \overline{\mathbb{Q}}$ and at least one is $\neq 0$, then actually $\gamma_1 \neq 0 \neq \gamma_2$. This implies $\frac{\log(\beta)}{\log(\alpha)} = -\frac{\gamma_1}{\gamma_2} \in \overline{\mathbb{Q}} \setminus \mathbb{Q}$, which is a contradiction to Corollary 4.1.4. □

Remark 4.1.6. In Corollary 4.1.5 (which is actually equivalent to Theorem 4.1.3) we have considered the homogeneous polynomial of degree one $x_1 \log(\alpha) + x_2 \log(\beta)$. But we called a homogeneous polynomial of degree one a linear form. So this is where the name of this chapter comes from.

As you may guess, the proof of the Gelfond-Schneider Theorem 4.1.3 requires some analysis. In particular, since we mix algebraic numbers α and β with $\alpha^\beta = e^{\beta \log(\alpha)}$, we may have to mix polynomials with the exponential function.

Definition 4.1.7. An *exponential polynomial* is a function on $\mathbb{C}$ of the form

$$R(z) = f_1(z)e^{\theta_1 z} + \ldots + f_N(z)e^{\theta_N z},$$

where $f_1, \ldots, f_N \in \mathbb{C}[x]$ are polynomials and $\theta_1, \ldots, \theta_N \in \mathbb{C}$.

As a finite sum of finite products of (the nicest) entire functions, any exponential polynomial is an entire function. It will turn out that for our purposes it is enough to consider exponential polynomials where all the polynomials are constant. We will make some easy observations.

Lemma 4.1.8. *Let $\theta_1, \ldots, \theta_N \in \mathbb{C}^*$ be pairwise distinct, and $b_1, \ldots, b_N \in \mathbb{C}$ be arbitrary. We consider the function $R(z) = b_1 e^{\theta_1 z} + \ldots + b_N e^{\theta_N z}$. Then*

(i) Some derivative of $R(z)$ is constantly zero if and only if $b_i = 0$ for all $i \in \{1, \ldots, N\}$.

(ii) If $R(z)$ is not constantly zero, then for all $s \in \mathbb{C}$ there is some derivative $R^{(k)}(z)$ of R such that $R^{(k)}(s) \neq 0$.

Proof. For completeness we mention that $R(z)$ (and all its derivatives) are constantly zero if all the b_i's are zero. For any $k \in \mathbb{N}_0$ the kth derivative of R is

$$\begin{aligned} R^{(k)}(z) &= b_1\theta_1^k e^{\theta_1 z} + \ldots + b_N\theta_N^k e^{\theta_N z} \\ &= b_1\theta_1^k \sum_{j\geq 0} \frac{1}{j!}\theta_1^j z^j + \ldots + b_N\theta_N^k \sum_{j\geq 0} \frac{1}{j!}\theta_N^j z^j \\ &= \sum_{j\geq 0} \frac{1}{j!} \left(\sum_{i=1}^N b_i \theta_i^{k+j} \right) z^j. \end{aligned} \tag{4.1}$$

By uniqueness of the power series representation of an entire function, if $R^{(k)}$ is constantly zero, then $\sum_{i=1}^N b_i\theta_i^{k+j} = 0$ for all $j \in \mathbb{N}_0$. In this case we have

$$\begin{pmatrix} \theta_1^{k+N-1} & \cdots & \theta_N^{k+N-1} \\ \vdots & \ddots & \vdots \\ \theta_1^k & \cdots & \theta_N^k \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_N \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Since $\theta_1, \ldots, \theta_N$ are pairwise distinct and non-zero, we know that the matrix on the left has full rank (Vandermonde!). Hence, this equality implies $b_1 = \ldots = b_N = 0$, which proves part (i).
Part (ii) is true for all entire functions. The Taylor expansion of R around $s \in \mathbb{C}$ is

$$R(z) = \sum_{j \geq 0} \frac{1}{j!} R^{(j)}(s)(z-s)^j. \tag{4.2}$$

Hence, if $R^{(k)}(s) = 0$ for all $k \in \mathbb{N}_0$, then $R(z)$ is constantly zero, proving part (ii). □

We also want to apply Cauchy's Interal Formula, which we recall here.

Theorem 4.1.9 (Cauchy's Integral Formula)**.** *Let $f : \mathbb{C} \to \mathbb{C}$ be an entire function. For any real $r > 0$, and a complex number w we set $D_r(w) = \{z \in \mathbb{C} | \, |z - w| \leq r\}$ and its boundary is denoted by $B_r(w) = \{z \in \mathbb{C} | \, |z - w| = r\}$. Then for any $v \in D_r(w)$ we have*

$$f(v) = \frac{1}{2\pi i} \int_{B_r(w)} \frac{f(z)}{z - v} \mathrm{d}z.$$

The last lemma that we source out of the proof is the following.

Lemma 4.1.10. *Let $\beta \in \overline{\mathbb{Q}}$ and $u, k \in \mathbb{N}$ be arbitrary. Then we have for any number field K of degree d containing β the estimate*

$$\prod_{v \in M_K} \max_{0 \leq a,b \leq u} \{1, |a + b\beta|_v^k\}^{d_v/d} \leq (2u)^k H(\beta)^k.$$

Proof. This is just a combination of the usual estimates for absolute values. If $v \in M_K$ is non-archimedean, we have

$$|a + b\beta|_v \leq \max\{|a|_v, |b|_v |\beta|_v\} \leq \max\{1, |\beta|_v\}.$$

If $v \in M_K$ is archimedean, then for all $a, b \in \{0, \ldots, u\}$ we have

$$|a + b\beta|_v \leq 2 \max\{|a|_v, |b|_v |\beta|_v\} \leq 2u \max\{1, |\beta|_v\}.$$

Using these estimates gives

$$\begin{aligned}
&\prod_{v \in M_K} \max_{0 \leq a,b \leq u} \{1, |a + b\beta|_v^k\}^{d_v/d} \\
\leq &\prod_{\substack{v \in M_K \\ v | \infty}} \max\{1, (2u)^k \max\{1, |\beta|_v^k\}\}^{d_v/d} \cdot \prod_{\substack{v \in M_K \\ v \nmid \infty}} \max\{1, \max\{1, |\beta|_v^k\}\}^{d_v/d} \\
\leq &(2u)^k \prod_{v \in M_K} \max\{1, \left|\beta^k\right|_v\}^{d_v/d} = (2u)^k H(\beta)^k.
\end{aligned}$$

□

Now we finally start the proof of the Gelfond-Schneider Theorem 4.1.3. Maybe you can recognize the strategy of the proof...

Proof of Theorem 4.1.3. We assume that α, β, and α^β are algebraic, with $\alpha \notin \{0,1\}$ and $\beta \notin \mathbb{Q}$. This will eventually lead to a contradiction. If all these elements are algebraic, there is some number field K containing all three elements. We set

$$d = [K : \mathbb{Q}],$$

and for computational reasons towards the end of the proof, we set

$$m = 6d + 2.$$

Next we fix an integer u, which is divisible by $2dm$, and define

$$N = u^2 \qquad \text{and} \qquad n = \frac{u^2}{2dm} > u.$$

This value of n will eventually tend to infinity. For all $(a,b) \in \{0,\dots,u-1\} \times \{1,\dots,u\}$ we define

$$\theta_{au+b} = \log(\alpha)(a + b\beta) \tag{4.3}$$

(for the bare definition, we need $\alpha \neq 0$). This gives $N = u^2$ values $\theta_1, \dots, \theta_N$, which are pairwise distinct, since

$$\begin{aligned} & \theta_{au+b} = \log(\alpha)(a+b\beta) = \log(\alpha)(a'+b'\beta) = \theta_{a'u+b'} \\ \iff \quad & a + b\beta = a' + b'\beta \\ \iff \quad & a = a' \quad \text{and } b = b'. \end{aligned}$$

The first equivalence sign follows since $\alpha \neq 1$ (and hence $\log(\alpha) \neq 0$), and the last equivalence sign follows since $\beta \notin \mathbb{Q}$. So, already now we have used all our assumptions on α and β.
In the following, the values $c_1, c_2, \dots$ denote absolute positive constants, which only depend on our given data α, β, α^β, and K (and on our choice of logarithm). We will several times use that m is given by these data, and hence we can use $c_i^m = c_{i+1}$. We begin with

$$u = c_1\sqrt{n}.$$

Let us now start with the interesting stuff!

1. step: the auxiliary (exponential) polynomial R.

We claim that there are $b_1, \dots, b_N \in \mathbb{Z}$, not all zero, such that the function

$$R(z) = b_1 e^{\theta_1 z} + \dots + b_N e^{\theta_N z}$$

satisfies

(i) $\log(\alpha)^{-k} R^{(k)}(s) = 0$ for all $(k,s) \in \{0,\dots,n-1\} \times \{1,\dots,m\}$, and

(ii) $|\gamma_i| \leq c_3^{n-1} n^{n+1/2}$ for all $i \in \{1,\dots,N\}$.

We replace the coefficients $b_1, \dots, b_N$ by variables $x_1, \dots, x_N$. We note that then the equations $\log(\alpha)^{-k} R^{(k)}(s) = 0$ are linear equations defined over K. Indeed, for any $(k,s) \in \{0, \dots, n-1\} \times \{1, \dots, m\}$ we define

$$\begin{aligned} L_{(k,s)}(\underline{x}) &= \log(\alpha)^{-k}(x_1\theta_1^k e^{\theta_1 s} + \dots + x_N \theta_N^k e^{\theta_N s}) \\ &\overset{\text{Def. of } \theta_i}{=} \sum_{a=0}^{u-1}\sum_{b=1}^{u} x_{au+b}(a+b\beta)^k e^{(a+b\beta)\log(\alpha)s} = \sum_{a=0}^{u-1}\sum_{b=1}^{u} x_{au+b}(a+b\beta)^k \alpha^{as}(\alpha^\beta)^{bs}, \end{aligned}$$

which is defined over K, since we assume $\alpha, \beta, \alpha^\beta \in K$. Moreover, (i) is satisfied, whenever $b_1, \dots, b_N$ is a solution of all the equations $L_{(k,s)}(\underline{x}) = 0$ for $(k,s) \in \{0, \dots, n-1\} \times \{1, \dots, m\}$ (cf. (4.1)). Hence, we are left with the problem of finding a small integral solution for the nm linear equations defined over K in N variables!
By our choices we have $N = 2dmn$, hence we can apply Siegel's Lemma 2.4.6. All that is left to do is to estimate the height of $L_{(k,s)}$. This is equal to

$$\begin{aligned} &\prod_{v \in M_K} \max_{\substack{0 \le a \le u-1 \\ 1 \le b \le u}} \{1, \left|(a+b\beta)^k \alpha^{as}(\alpha^\beta)^{bs}\right|_v\}^{d_v/d} \\ &\le \prod_{v \in M_K} \max_{\substack{0 \le a \le u-1 \\ 1 \le b \le u}} \{1, |a+b\beta|_v^k\}^{d_v/d} \cdot \prod_{v \in M_K} \max_{0 \le a \le u-1} \max\{1, |\alpha|_v^{as}\}^{d_v/d} \cdot \prod_{v \in M_K} \max_{1 \le b \le u} \{1, \left|\alpha^\beta\right|_v^{bs}\}^{d_v/d} \\ &\overset{4.1.10}{\le} (2u)^k H(\beta)^k \cdot H(\alpha)^{(u-1)s} \cdot H(\alpha^\beta)^{us} \\ &\le (2u)^{n-1} H(\beta)^{n-1} (H(\alpha)H(\alpha^\beta))^{um} \\ &\overset{u<n}{\le} (2c_1)^{n-1} n^{n-1/2} H(\beta)^{n-1} ((H(\alpha)H(\alpha^\beta))^m)^{n-1} = c_2^{n-1} n^{n-1/2}. \end{aligned}$$

By Siegel's Lemma 2.4.6 we conclude, that there are $b_1, \dots, b_N \in \mathbb{Z}$, not all zero, such that (i) is satisfied and such that

$$\max_{1 \le i \le N} |b_i| \le (N c_2^{n-1} n^{n-1/2})^{\frac{dmn}{N-dmn}} = c_1^2 n c_2^{n-1} n^{n-1/2} \le c_3^{n-1} n^{n+1/2}.$$

This proves the claim.

From now on we set $R(z) = b_1 e^{\theta_1 z} + \dots + b_N e^{\theta_N z}$ such that (i) and (ii) from above are satisfied!

2. step: the helpful value λ.

We know from Lemma 4.1.8 that for any $s \in \mathbb{C}$ there is some derivative of R which does not vanish at s. Hence, using the first step, we know that there is some $r \ge n$ and some $s' \in \{1, \dots, m\}$ such that

$$R^{(r)}(s') \neq 0 \quad \text{and} \quad R^{(k)}(s) = 0 \quad \forall (k,s) \in \{1, \dots, r-1\} \times \{1, \dots, m\}.$$

This just means that r is the smallest integer for which $R^{(r)}$ vanishes at some point $s' \in \{1, \dots, m\}$. From the first step, we know indeed that

$$r \ge n.$$

We conclude that

$$\lambda = (\log(\alpha))^{-r} R^{(r)}(s') = \sum_{a=0}^{u-1} \sum_{b=1}^{u} b_{au+b}(a+b\beta)^r \alpha^{as'} (\alpha^\beta)^{bs'} \tag{4.4}$$

is a non-zero element in K.

3. step: bounding the size of λ from below.

As we know there are several different ways of measuring the size of an algebraic number. This time, we use the *norm* of λ. To this end, we let $c_4 \in \mathbb{N}$ be such that $c_4\beta \in \mathcal{O}_K$, $c_4\alpha \in \mathcal{O}_K$, and $c_4\alpha^\beta \in \mathcal{O}_K$. In particular, we have

$$c_4^r(a+b\beta)^r \in \mathcal{O}_K \quad \forall\ (a,b) \in \{0,\dots,u-1\} \times \{1,\dots,u\}.$$

Using $s' \leq m$, we also find

$$c_4^{2um}\alpha^{as'}(\alpha^\beta)^{bs'} \in \mathcal{O}_K \quad \forall\ (a,b) \in \{0,\dots,u-1\} \times \{1,\dots,u\}.$$

Hence, $c_4^{r+2um}\lambda \in \mathcal{O}_K$. This implies

$$c_4^{d(r+2um)} \left|N_{K/\mathbb{Q}}(\lambda)\right| = \left|N_{K/\mathbb{Q}}(c_4^{r+2um}\lambda)\right| \geq 1.$$

Since $c_4 \geq 1$ and $r \geq n \geq u$, this implies

$$\left|N_{K/\mathbb{Q}}(\lambda)\right| \geq c_4^{-d(r+2um)} \geq c_4^{-d(r+2mr)} = c_5^r. \tag{4.5}$$

4. step: bounding the size of λ from above.

Let us first calculate a bound for any factor appearing in the product defining $N_{K/\mathbb{Q}}(\lambda)$. We chose any archimedean $v \in M_K$ and get

$$|\lambda|_v \leq N \cdot \max_{\substack{0\leq a\leq u-1\\ 1\leq b\leq u}} \left|b_{au+b}(a+b\beta)^r\alpha^{as'}(\alpha^\beta)^{bs'}\right|_v = N \cdot \max_{1\leq i\leq N}|b_i| \cdot \max_{\substack{0\leq a\leq u-1\\ 1\leq b\leq u}} \left|(a+b\beta)^r\alpha^{as'}(\alpha^\beta)^{bs'}\right|_v.$$

A bound for the absolute value of b_i has been calculated in the first step, and the last factor can be bounded by the same methods as in Lemma 4.1.10. This yields (using once again $s' \leq m$)

$$\begin{aligned}
|\lambda|_v &\leq N c_3^{n-1} n^{n+1/2} (2u)^r \max\{1,|\beta|_v\}^r \left(\max\{1,|\alpha|_v\}^m \max\{1,\left|\alpha^\beta\right|_v\}^m\right)^u \\
&\overset{N=u^2}{=} c_3^{n-1} n^{n+1/2} u^{r+2} c_6^r c_7^u \\
&\overset{r\geq n\geq u}{\leq} c_8^r r^{r+1/2} u^{r+2} \overset{u\leq c_1\sqrt{r}}{=} c_9^r r^{2r+3/2}.
\end{aligned}$$

In particular, we have that the largest factor appearing in $N_{K/\mathbb{Q}}$ is less or equal to this value. Hence

$$\left|N_{K/\mathbb{Q}}(\lambda)\right| \leq \left(c_9^r r^{2r+3/2}\right)^{d-1} \cdot |\lambda| = c_{10}^r r^{(d-1)(2r+3)/2} \cdot |\lambda|. \tag{4.6}$$

We are left to prove that $|\lambda|$ is very small.
The function $R(z)$ has order at least r at all points in $\{1,\dots,m\}$. Hence the function

$$T(z) = r!\frac{R(z)}{(z-s')^r}\prod_{j\in\{1,\dots,m\}\setminus\{s'\}}\left(\frac{s'-j}{z-j}\right)^r$$

has no poles. Thus T is an entire function. That T might be helpful becomes clear if we consider the Taylor expansion of R around s'. This is

$$\begin{aligned}
& R(z) = \sum_{j\geq 0}\frac{1}{j!}R^{(j)}(s')(z-s')^j = \sum_{j\geq r}\frac{1}{j!}R^{(j)}(s')(z-s')^j \\
\implies\ & T(z) = r!\left(\sum_{j\geq r}R^{(j)}(s')(z-s')^{j-r}\right)\prod_{j\in\{1,\dots,m\}\setminus\{s'\}}\left(\frac{s'-j}{z-j}\right)^r \\
\implies\ & T(s') = r!\frac{1}{r!}R^{(r)}(s') \overset{(4.4)}{=} \log(\alpha)^r\lambda. \qquad (4.7)
\end{aligned}$$

We apply the Cauchy Integral Formula 4.1.9 for T, $D_{m(1+\frac{r}{u})}(0)$, and s' (note that indeed $s' \in D_{m(1+\frac{r}{u})}(0)$) to get

$$\lambda \overset{(4.7)}{=} \log(\alpha)^{-r}T(s') = \log(\alpha)^{-r}\frac{1}{2\pi i}\int_{B_{m(1+\frac{r}{u})}(0)}\frac{T(z)}{z-s'}\mathrm{d}z. \qquad (4.8)$$

From now on let $z \in B_{m(1+\frac{r}{u})}(0)$; i.e. $|z| = m(1+\frac{r}{u})$. Then we have

$$\begin{aligned}
|R(z)| &\leq N\cdot\max_{1\leq i\leq N}|b_i|\cdot\left|e^{\theta_i z}\right| \leq u^2c_3^{n-1}n^{n+1/2}\max_{1\leq i\leq N}e^{|\theta_i z|} \\
&\overset{(ii)}{\leq} u^2c_3^{n-1}n^{n+1/2}\left(\max_{1\leq i\leq N}e^{|\theta_i|}\right)^{m(1+\frac{r}{u})} \\
&\overset{u^2=c_1^2n}{\leq} c_{11}^{n-1}n^{n+3/2}\left(\max_{1\leq i\leq N}e^{|\log(\alpha)||a+b\beta|}\right)^{m(1+\frac{r}{u})} \\
&\leq c_{11}^{n-1}n^{n+3/2}\left(\max_{1\leq i\leq N}e^{|\log(\alpha)|\max\{1,|\beta|\}}\right)^{mu(1+\frac{r}{u})} \\
&\leq c_{11}^{n-1}n^{n+3/2}c_{12}^{u+r} \\
&\overset{u\leq n\leq r}{\leq} c_{13}^{2r}r^{r+3/2},
\end{aligned}$$

and

$$|z-k| \geq |z| - k = m(1+\frac{r}{u}) - k \geq \frac{rm}{u} \quad \forall\ k\in\{1,\dots,m\}. \qquad (4.9)$$

Combining these two estimates with the definition of T, gives

$$\begin{aligned}
|T(z)| &\leq r! \frac{|R(z)|}{|z-s'|^r} \prod_{j\in\{1,\dots,m\}\setminus\{s'\}} \left(\frac{|s'-j|}{|z-j|}\right)^r \\
&\leq r! c_{13}^{2r} r^{r+3/2} \left(\frac{rm}{u}\right)^{-r} \prod_{j\in\{1,\dots,m\}\setminus\{s'\}} \left(\frac{m}{rm/u}\right)^r \\
&= r! c_{13}^{2r} r^{r+3/2} \frac{u^r}{r^r m^r} \frac{u^{r(m-1)}}{r^{r(m-1)}} \\
&\overset{r!\leq r^r}{\leq} c_{14}^{2r} r^{r+3/2} u^{rm} r^{-r(m-1)} \\
&\overset{u\leq c_1\sqrt{r}}{\leq} c_{15}^{2r} r^{r+3/2-r(m-1)+rm/2} = c_{15}^{2r} r^{r(3-m)+3/2}. \qquad (4.10)
\end{aligned}$$

Plugging this into (4.8) yields

$$\begin{aligned}
|\lambda| &\leq |\log(\alpha)|^{-r}\, m(1+\frac{r}{u}) c_{15}^{2r} r^{r(3-m)+3/2} \cdot \frac{u}{rm} \leq c_{16}^r \underbrace{(\frac{u}{r}+1)}_{\leq u\leq c_1\sqrt{r}} r^{r(3-m)+3/2} \\
&\leq c_{17}^r r^{r(3-m)+4/2},
\end{aligned}$$

and with the aid of (4.6) we conclude

$$\left|N_{K/\mathbb{Q}}(\lambda)\right| \leq c_{10}^r r^{(d-1)(2r+3)/2} \cdot c_{17}^r r^{r(3-m)+4/2}.$$

Now finally our weird choice of m (which was up to now completely irrelevant) comes into play. Note that for large m the norm of λ becomes particularly small. However, we cannot let m tend to infinity, since throughout we have used heavily, that m is a constant only depending on K. However, we have chosen m right at the beginning so that the following bound is true:

$$\left|N_{K/\mathbb{Q}}(\lambda)\right| \leq c_{18}^r r^{-r}. \qquad (4.11)$$

5. step: Comparison.

By (4.5) and (4.11), we have

$$c_5^r \leq c_{18}^r r^{-r} \quad \Longrightarrow \quad r \leq c_{18}/c_5$$

for positive constants c_5 and c_{18} only depending on K. In particular, c_5 and c_{18} are independent on n. Now, if we perform all these computations with some $n \geq c_{18}/c_5$, then also $r \geq n \geq c_{18}/c_5$, which gives a contradiction!
Hence, we must have made a wrong assumption. This means that α^β cannot be algebraic! □

A deep generalization of the Gelfond-Schneider Theorem 4.1.3 is the following theorem due to Alan Baker.

Theorem 4.1.11 (Baker, 1966)**.** *Let $\alpha_1,\dots,\alpha_n \in \overline{\mathbb{Q}}^*$. If $\log(\alpha_1),\dots,\log(\alpha_n)$ are $\mathbb{Q}$-linearly independent, and $\gamma_0,\gamma_1,\dots,\gamma_n \in \overline{\mathbb{Q}}$ are not all equal to zero, then*

$$\gamma_0 + \gamma_1\log(\alpha_1) + \dots + \gamma_n\log(\alpha_n) \neq 0.$$

This is, not only $\log(\alpha_1), \ldots, \log(\alpha_n)$ are $\overline{\mathbb{Q}}$-algebraic independent as soon as they are $\mathbb{Q}$-linearly independent, but also $1, \log(\alpha_1), \ldots, \log(\alpha_n)$ are $\overline{\mathbb{Q}}$-linearly independent. At this point you should ask yourself whenever something is not equal to zero: Is it bounded away from zero?
The following effective version of the last theorem is also due to Alan Baker and it answers this question.

Theorem 4.1.12. *Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^*$. If $\log(\alpha_1), \ldots, \log(\alpha_n)$ are $\mathbb{Q}$-linearly independent, and $\gamma_0, \gamma_1, \ldots, \gamma_n \in \overline{\mathbb{Q}}$ are not all equal to zero, then*

$$|\gamma_0 + \gamma_1 \log(\alpha_1) + \ldots + \gamma_n \log(\alpha_n)| \geq (eB)^{-c},$$

where $B = \max_{0 \leq i \leq n}(2H(\gamma_i))^{\deg(\gamma_i)}$ and $c \geq 1$ only depends on n and $\alpha_1, \ldots, \alpha_n$.

4.2 Applications

4.2.1 Transcendence

As seen in the last section, these linear forms in logarithms are closely related to results on transcendental number.

Proposition 4.2.1. *Let $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^*$ and $\gamma_1, \ldots, \gamma_n \in \overline{\mathbb{Q}}$. Then*

$$\gamma_1 \log(\alpha_1) + \ldots + \gamma_n \log(\alpha_n)$$

is either zero or transcendental.

Proof. We want to prove this by induction on n. So we start with $n = 1$, and let $\alpha_1 \in \overline{\mathbb{Q}}^*$ and $\gamma_1 \in \overline{\mathbb{Q}}$ be arbitrary. If $\alpha_1 = 1$ or $\gamma_1 = 0$, then $\gamma_1 \log(\alpha_1) = 0$. Hence, we assume that $\alpha_1 \in \overline{\mathbb{Q}}^* \setminus \{1\}$ and $\gamma_1 \in \overline{\mathbb{Q}}^*$, and show that $\gamma_1 \log(\alpha_1)$ is transcendental. But, since $\gamma_1 \in \overline{\mathbb{Q}}^*$, this last number is transcendental, if and only if $\log(\alpha_1)$ is transcendental. But this follows from the Lindemann-Weierstraß Theorem (see Example 4.1.2). This proves the Proposition for $n = 1$.
Now we fix some $n \in \mathbb{N}$ and assume that the statement is correct for n. Then we have to prove the statement for $n + 1$.
Assume the statement is incorrect for $n + 1$. Then there are elements $\alpha_1, \ldots, \alpha_{n+1} \in \overline{\mathbb{Q}}^*$ and $\gamma_1, \ldots, \gamma_{n+1} \in \overline{\mathbb{Q}}^*$ such that

$$\begin{aligned} & \gamma_1 \log(\alpha_1) + \ldots + \gamma_{n+1} \log(\alpha_{n+1}) = \gamma_0 \in \overline{\mathbb{Q}}^* \\ \iff \quad & (-\gamma_0) + \gamma_1 \log(\alpha_1) + \ldots + \gamma_{n+1} \log(\alpha_{n+1}) = 0. \end{aligned} \tag{4.12}$$

By Theorem 4.1.11 we know that $\log(\alpha_1), \ldots, \log(\alpha_{n+1})$ are $\mathbb{Q}$-linearly dependent. This is, there are rational numbers $c_1, \ldots, c_{n+1}$ not all zero, such that

$$c_1 \log(\alpha_1) + \ldots + c_{n+1} \log(\alpha_{n+1}) = 0.$$

After possibly renumbering the elements, we may assume that $c_{n+1} \neq 0$. Then we get

$$\log(\alpha_{n+1}) = -\frac{c_1}{c_{n+1}} \log(\alpha_1) - \ldots - \frac{c_n}{c_{n+1}} \log(\alpha_n). \tag{4.13}$$

We plug (4.13) into (4.12) and get

$$\underbrace{(\gamma_1 - \frac{c_1}{c_{n+1}}\gamma_{n+1})}_{\in\overline{\mathbb{Q}}}\log(\alpha_1) + \ldots + \underbrace{(\gamma_n - \frac{c_n}{c_{n+1}}\gamma_{n+1})}_{\in\overline{\mathbb{Q}}}\log(\alpha_n) = \gamma_0 \in \overline{\mathbb{Q}}^*.$$

This contradicts our induction hypothesis, which states that $(\gamma_1 - \frac{c_1}{c_{n+1}}\gamma_{n+1})\log(\alpha_1) + \ldots + (\gamma_n - \frac{c_n}{c_{n+1}}\gamma_{n+1})\log(\alpha_n)$ is either zero or transcendental. This proves the proposition. □

Remark 4.2.2. The very same induction also proves that $\gamma_1\log(\alpha_1) + \ldots + \gamma_n\log(\alpha_n)$ is always non-zero (and thus transcendental), when $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^* \setminus \{1\}$ and $\gamma_1, \ldots, \gamma_n \in \overline{\mathbb{Q}}^*$ are $\mathbb{Q}$-linearly independent.

We want to derive a multiplicative version of Proposition 4.2.1. Before we give the statement, we should once again mention that our logarithm log depends on a choice. In particular, the expected equality $\log(z \cdot w) = \log(z) + \log(w)$ may not be true. This is due to the fact that although $e^{\log(z)} = z$ for all $z \in \mathbb{C}^*$, the equality $\log(e^z) = z$ is only true up to some element in $(2\pi i)\mathbb{Z}$. This essentially proves the next lemma.

Lemma 4.2.3. *The following statements hold true.*

(a) For all $z, w \in \mathbb{C}^*$ there exists a $k \in \mathbb{Z}$ such that $\log(zw) = \log(z) + \log(w) + (2\pi i)k$.

(b) For all $z, w \in \mathbb{C}$, with $z \neq 0$, there exists a $k' \in \mathbb{Z}$ such that $\log(z^w) = w\log(z) + (2\pi i)k'$.

(c) We have $\log(-1) = \pi i(1 + 2\ell)$ for some $\ell \in \mathbb{Z}$.

Proof. We start with proving (a). It is

$$\log(zw) = \log(e^{\log(z)}e^{\log(w)}) = \log(e^{\log(z)+\log(w)}) = (\log(z) + \log(w)) + (2\pi i)k$$

for some $k \in \mathbb{Z}$.
Part (b) comes from the definition of z^w, since this gives

$$\log(z^w) = \log(e^{w\log(z)}) = w\log(z) + (2\pi i)k'$$

for some $k' \in \mathbb{Z}$.
Finally, part (c) follows from Euler's formula $-1 = e^{\pi i}$, since this yields

$$\log(-1) = \log(e^{\pi i}) = (\pi i) + 2\pi i\ell = (\pi i)(1 + 2\ell)$$

for some $\ell \in \mathbb{Z}$. □

Corollary 4.2.4. *Let $\gamma_0, \alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^*$ and $\gamma_1, \ldots, \gamma_n \in \overline{\mathbb{Q}}$ be arbitrary. Then*

$$e^{\gamma_0}\alpha_1^{\gamma_1} \cdots \alpha_n^{\gamma_n}$$

is transcendental.

Proof. Our assumptions guarantee that $\alpha_{n+1} = e^{\gamma_0}\alpha_1^{\gamma_1}\cdots\alpha_n^{\gamma_n}$ is non-zero. From Lemma 4.2.3 we conclude

$$\begin{aligned}\log(\alpha_{n+1}) &= \gamma_0 + \gamma_1\log(\alpha_1) + \ldots + \gamma_n\log(\alpha_n) + (2\pi i)k \\ &= \gamma_0 + \gamma_1\log(\alpha_1) + \ldots + \gamma_n\log(\alpha_n) + \frac{2k}{1+2\ell}\log(-1)\end{aligned}$$

for some $k, \ell \in \mathbb{Z}$. Reformulating this gives

$$\gamma_1\log(\alpha_1) + \ldots + \gamma_n\log(\alpha_n) + \frac{2k}{1+2\ell}\log(-1) + (-1)\log(\alpha_{n+1}) = -\gamma_0 \in \overline{\mathbb{Q}}^*.$$

Now Proposition 4.2.1 tells us that at least one of $-1, \alpha_1, \ldots, \alpha_{n+1}$ is transcendental (otherwise, the last equation would be either zero or a transcendental number, what is not the case). But we know that $\alpha_1, \ldots, \alpha_n$ are algebraic (and so is -1). Hence, $\alpha_{n+1} = e^{\gamma_0}\alpha_1^{\gamma_1}\cdots\alpha_n^{\gamma_n}$ is transcendental. □

Remark 4.2.5. Note that in the last corollary it is essential that $\gamma_0 \neq 0$. Otherwise, you can easily construct counterexamples. For instance, if $\gamma_1, \ldots, \gamma_n$ are all rational numbers, then surely $\alpha_1^{\gamma_1}\cdots\alpha_n^{\gamma_n} \in \overline{\mathbb{Q}}^*$. Or, if $\alpha_1 = \alpha_2 \in \overline{\mathbb{Q}}^*$, then for all $\gamma \in \overline{\mathbb{Q}}^*$ we have $\alpha_1^{\gamma}\cdot\alpha_2^{-\gamma} = 1 \in \overline{\mathbb{Q}}^*$. However, with some mild extra restrictions on the α_i's and/or the γ_i's, one can prove that $\alpha_1^{\gamma_1}\cdots\alpha_n^{\gamma_n}$ is transcendental. A sloppy (but true) formulation of this reads: For $\alpha_1, \ldots, \alpha_n, \gamma_1, \ldots, \gamma_n \in \overline{\mathbb{Q}}$, the number $\alpha_1^{\gamma_1}\cdots\alpha_n^{\gamma_n}$ is either algebraic for trivial reasons, or it is transcendental.

Now, you have some tools at hand to write down arbitrarily many complex numbers, which are transcendental. For instance: $e^2\cdot 3^{\sqrt{5}}$, $7\pi + \log(11)$, $13\log(17) + 19\log(23) + 29\log(31)$, ... Speaking about prime numbers, let us move from transcendental number theory to other applications of linear forms in logarithms. The rest of this section will be mainly a summary of results, without giving the proofs. All proofs and many more information on this topic can be found in [3] and [9].

4.2.2 Prime Divisors of Polynomial Values

I indicated, that we now want to speak about prime numbers. So let us use the following notation.

Notation 4.2.6. For any $n \in \mathbb{Z}\setminus\{-1, 0, 1\}$ we denote with $P[n]$ the largest prime number that divides n. Moreover, we set $P[-1] = P[0] = P[1] = 1$.

Using linear forms in logarithms one can prove the following theorem.

Theorem 4.2.7. *Let $f(x) \in \mathbb{Z}[x]\setminus\{0\}$ be a polynomial with at least two different roots. Then there exists a constant $C(f)$ only depending on f, such that for all $k \geq 100$ we have*

$$P[f(k)] \geq C(f)\log\log(k). \tag{4.14}$$

Before we explain the connection to linear forms in logarithms, let us try to understand this result. It tells us in particular that the largest prime divisor of $f(n)$ tends to infinity, as n tends to infinity (if f has at least two distinct roots).

Remark 4.2.8. The assumption on the number of roots is indeed necessary: If $f(x) \in \mathbb{Z}[x]$ has only one root, then $f(x) = a(bx+c)^d$ for $a, b, c, d \in \mathbb{Z}$, with $a \neq 0$, and $b, d \geq 1$. Assume first that $c = 0$, then for all $n \in \mathbb{N}$ we have

$$P[f(2^n)] = P[ab^d 2^{dn}] = \max\{P[a], P[b], 2\}.$$

In particular, (4.14) cannot be satisfied. Similarly, if $c > 0$ for all $n \in \mathbb{N}$ we can plug $\frac{((b+1)^n-1)c}{b}$ (which is in $\mathbb{N}$) into f and get

$$P[f(\frac{((b+1)^n-1)c}{b})] = P[a(b+1)^{dn}c^d] = \max\{P[a], P[b+1], c\}.$$

Since $\frac{((b+1)^n-1)c}{b}$ tends to infinity, if n tends to infinity, again (4.14) cannot be satisfied. A similar counterexample works if $c < 0$.

We want to apply a multiplicative version of Baker's Theorem 4.1.12. To ease notation we will only consider the special case where the numbers $\gamma_0, \ldots, \gamma_n$ are rational integers, and also that $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}$ are positive real numbers. Then we may assume that the logarithm is the usual logarithm on the positive real numbers. We recall the *Mercator series*.

Lemma 4.2.9. *Let* log *be the usual natural logarithm on the positive real numbers. Then for all* $x \in (-1, 1)$ *we have* $\log(1+x) = \sum_{n\geq 1} \frac{(-1)^{n+1}}{n} x^n$.

Proof. All we have to do is to calculate the Taylor expansion of $\log(1+x)$ around 0. The first derivative of $\log(1+x)$ is $\log(1+x)^{(1)} = \frac{1}{1+x}$. The other derivatives are of course easily calculated: $\log(1+x)^{(2)} = (-1)\frac{1}{(1+x)^2}$, $\log(1+x)^{(3)} = (-1)(-2)\frac{1}{(1+x)^3}$, $\log(1+x)^{(4)} = (-1)(-2)(-3)\frac{1}{(1+x)^4}$, and hence $\log(1+x)^{(n)} = (-1)^{n+1}(n-1)!\frac{1}{(1+x)^n}$ for all $n \in \mathbb{N}$. Now the Taylor expansion of $\log(1+x)$ around 0 is

$$\log(1+x) = \log(1+0) + \frac{1}{1!}x + \frac{(-1)1!}{2!}x^2 + \frac{2!}{3!}x^3 + \ldots = \sum_{n\geq 1} \frac{(-1)^{n+1}}{n} x^n.$$

The radius of convergence is $\lim_{n\to\infty} \left|\frac{1/n}{1/(n+1)}\right| = \lim_{n\to\infty} \left|\frac{n+1}{n}\right| = 1$. This proves the lemma. □

Theorem 4.2.10. *Let* $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^*$ *be positive real numbers such that* $\log(\alpha_1), \ldots, \log(\alpha_n)$ *are* $\mathbb{Q}$*-linearly independent, and* $\gamma_1, \ldots, \gamma_n \in \mathbb{Z}$ *be not all zero. Then*

$$|\alpha_1^{\gamma_1} \cdots \alpha_n^{\gamma_n} - 1| \geq (eB)^{-c'},$$

where $B = \max_{1\leq i\leq n}(2H(\gamma_i))^{\deg(\gamma_i)}$ *and* $c' \geq 1$ *only depends on* n *and* $\alpha_1, \ldots, \alpha_n$.

Proof. Since we are working on the positive real numbers, for this proof we use the usual logarithm instead of an arbitrarily chosen branch. If $|\alpha_1^{\gamma_1} \cdots \alpha_n^{\gamma_n} - 1| \geq 1/2$, then the statement of the theorem is trivially satisfied. Hence, we may assume from now on that $|\alpha_1^{\gamma_1} \cdots \alpha_n^{\gamma_n} - 1| < 1/2$. We abbreviate $x = \alpha_1^{\gamma_1} \cdots \alpha_n^{\gamma_n} - 1$. Then, by the preceding lemma, we have

$$|\log(1+x)| = \left|\sum_{n\geq 1} \frac{(-1)^{n+1}}{n} x^n\right| < \sum_{n\geq 1} \frac{1}{n} |x|^n = |x| \sum_{n\geq 1} \frac{1}{n} |x|^{n-1} < |x| \sum_{n\geq 0} (\frac{1}{2})^n = 2|x|.$$

On the other hand we have

$$|\log(1+x)| = |\log(\alpha_1^{\gamma_1} \cdots \alpha_n^{\gamma_n})| = \left| \sum_{i=1}^{n} \gamma_i \log(\alpha_i) \right| \overset{4.1.12}{\geq} (eB)^{-c},$$

with B, c as in the statement of the theorem. Combining these estimates, we find

$$|x| \geq \frac{1}{2}(eB)^{-c} \geq (eB)^{-(c+\log(2))}.$$

Thus, the theorem follows with $c' = c + \log(2)$. □

Remark 4.2.11. A constant c' that satisfies the statement of Theorem 4.2.10 can actually perfectly explicit be written down. I will not bother you with the long expression for the best possible choice, but we will need some further knowledge on how c' depends on n and $\alpha_1, \ldots, \alpha_n$. To this end, we will give a possible choice for c' if $\alpha_1, \ldots, \alpha_n \in \mathbb{N} \setminus \{1\}$, and $n \geq 2$. Then, a possible choice for c' such that Theorem 4.2.10 is fulfilled is

$$c' = 300000^n \log(\alpha_1) \cdots \log(\alpha_n).$$

The general bound looks similar, but there is a further dependence on the degree of the number field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

4.2.12. Let us now finally come back to Theorem 4.2.7. We will only prove the theorem for the specific polynomial $f(x) = x(x+1)$. This is somehow the simplest polynomial with at least two different roots. However, it should give us an idea on how linear forms in logarithms are involved.
Denote by p_i the ith prime number; i.e. $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, and so on. By the prime number theorem 2.5.5 we know that p_i is essentially of size $i \log(i)$ for all $i \in \mathbb{N}$. More concretely, there is an absolute constant c_1 such that $p_i \leq c_1 i \log(i)$ for all $i \geq 2$.
Let $k \in \mathbb{N}$ be any large integer, and let

$$f(k) = k(k+1) = p_1^{e_1} \cdots p_n^{e_n}$$

be the prime power factorization of $f(k)$, with $e_1, \ldots, e_n \in \mathbb{N}_0$, and $e_n \neq 0$. This implies in particular that $P[f(k)] = p_n$. Since k and $k+1$ are coprime, there is a proper subset $I \subset \{1, \ldots, n\}$ such that

$$k = \prod_{i \in I} p_i^{e_i} \qquad \text{and} \qquad (k+1) = \prod_{i \in \{1,\ldots,n\} \setminus I} p_i^{e_i}.$$

For all $i \in \{1, \ldots, n\}$ we define

$$\epsilon_i = \begin{cases} -1 & \text{if } i \in I \\ 1 & \text{if } i \notin I. \end{cases}$$

Then we have

$$\frac{1}{k} = \frac{k+1}{k} - 1 = |p_1^{\epsilon_1 e_1} \cdots p_n^{\epsilon_n e_n} - 1|. \tag{4.15}$$

Haven't we seen this just now? So here comes the theory of linear forms in logarithms into play. We apply Theorem 4.2.10 with the bound given in Remark 4.2.11, to conclude

$$\frac{1}{k} \geq \left(2e \max_{1 \leq i \leq n} e_i \right)^{-300000^n \log(p_1) \cdots \log(p_n)}. \tag{4.16}$$

Note that surely we have $n \geq 2$. Now, for any $i \in \{1, \ldots, n\}$ we either have $p_i^{e_i} \mid k$ or $p_i^{e_i} \mid k+1$. Hence, in any case we have

$$2^{e_i} \leq p_i^{e_i} \leq k+1 \quad \Longrightarrow \quad \log(2) \max_{1 \leq i \leq n} e_i \leq \log(k+1) \leq 2\log(2)\log(k).$$

The last inequality easily follows by noting that $k \geq 100$. By plugging this into (4.16), taking logarithms, and multiply by -1 we get

$$\begin{aligned}\log(k) &\leq 300000^n \log(p_1) \cdots \log(p_n) \cdot \log(4e\log(k)) \\ &\leq 300000^n \log(p_n)^n \cdot \log(4e\log(k)) \\ &\leq 300000^n \log(c_1 n \log(n))^n \cdot \log(4e\log(k)) \\ &\leq 300000^n \log(c_1 n \log(n))^n \cdot 2\log\log(k).\end{aligned}$$

Note that if k increases, then also n has to increase! But, recall that $P[f(k)] = p_n$ is the nth prime number. Hence, if k tends to infinity, then $P[f(k)]$ tends to infinity as well.
In order to justify the claimed bound $P[f(k)] \geq C(f)\log\log(n)$, we get rid of all explicit constants. Note that for some absolute constant c_2 we have $\log(c_1 n \log(n)) \leq c_2^{\log\log(n)}$ for $n \geq 3$ (the case $n = 2$ can be handled, by either introduce another constant, or by choosing k large enough). Hence, the last inequality, may be written as

$$\log(k) \leq c_4^{n\log\log(n)} \log\log(k).$$

for some absolute constant c_4. This implies

$$n\log(n) \geq n\log\log(n) \geq \frac{1}{\log(c_4)}(\log\log(k) - \log\log\log(k)) \geq \frac{1}{2\log(c_4)}\log\log(k).$$

Since again by the prime number theorem 2.5.5 we have that $n\log(n)$ is essentially equal to p_n, Theorem 4.2.7 (for $f(x) = x(x+1)$) is proved.

4.2.3 Differences of Perfect Powers

Example 4.2.13. How many pairs of powers of 2 and powers of 3 have a difference of at most 10? Of course we can trivially answer this question for any fixed power of 3 (or fixed power of 2).

- the only powers of 2 which differ from 3^1 by at most 10 are: 2^1, 2^2, 2^3.
- the only powers of 2 which differ from 3^2 by at most 10 are: 2^1, 2^2, 2^3, 2^4.
- the only power of 2 which differ from 3^3 by at most 10 is: 2^5.
- there are no powers of 2 which differ from 3^4 by at most 10.

Using this trivial approach one can never answer this question in general, since there *might* be a ridiculously large n such that there is a power of 2 close to 3^n. We use linear forms in logarithms, to explain why there is actually no such large n.

Let $n \in \mathbb{N}$ be arbitrary and assume that there is some $m \in \mathbb{N}$ such that $|2^m - 3^n| \leq 10$. Then there exists a $k \in \mathbb{Z} \setminus \{0\}$, with $|k| \leq 10$, such that $2^m + k = 3^n$. Hence, we are actually dealing with Diophantine equations.
The polynomial $f_k(x) = x(x-k)$ has two distinct roots, and therefore by Theorem 4.2.7 we have for all $n \geq 5$ (since this implies $3^n \geq 100$).

$$P[f_k(3^n)] \geq C(f_k) \log\log(3^n).$$

But on the other hand

$$P[f_k(3^n)] = P[3^n(3^n - k)] = P[3^n 2^m] = 3.$$

Hence, $C(f_k) \log\log(3^n) \leq 3$ for an explicitly given constant $C_k(f)$. This gives

$$\log(n) \leq \frac{3}{C(f_k)} - \log\log(3).$$

This is nothing but an upper bound for n only depending on k. By considering this inequality for all $k \in \mathbb{Z} \setminus \{0\}$ with $|k| \leq 10$, gives an upper bound for n only depending on 10. According to Example 4.2.13 there are only finitely many further cases to check. Making the calculations explicit (calculating $C(f_k)$ and checking the finitely many possible powers of 3) gives, that there is no further pair of powers of 2 and powers of 3 which differ by at most 10.
Of course, we can replace 2, 3, and 10 by essentially any numbers. Then we get.

Theorem 4.2.14. *Let $a, b, k \in \mathbb{N}$ be such that $a^n \neq b^m$ for all $m, n \in \mathbb{N}$. Then the number of pairs $(m, n) \in \mathbb{N}^2$ such that $|a^n - b^m| \leq k$ is finite and can be explicitly determined.*

4.2.4 The Thue Equation

The last application of the theory of linear forms in logarithms which we mention, is an *effective* solution of Thue equations (see Theorem 3.1.3). This claimed effectiveness is a bound on the size of a solution to a given Thue equation. We restrict to the case of an integral solution.

Theorem 4.2.15. *Let $F \in \mathbb{Z}[x, y]$ be homogeneous with pairwise distinct linear factors, of degree $d \geq 3$, and let $m \in \mathbb{Z} \setminus \{0\}$. Then there exists a positive real number C, which can be calculated only in terms of F, such that all pairs $(a, b) \in \mathbb{Z}^2$ that satisfy $F(a, b) = m$, also satisfy $\max\{|a|, |b|\} \leq |2m|^C$.*

This result obviously implies that the equation $F(x, y) = m$ has at most finitely many solutions. But it is actually much better than that. In principle, one (okay: a PC) could test all pairs $(a, b) \in \mathbb{Z}^2$ with $\max\{|a|, |b|\} \leq |2m|^C$, whether it is a solution to the equation $F(x, y) = m$ or not. Then, we would have found indeed all integral solutions to a Thue equation. Nowadays, it is actually not hard for a PC to give all solutions to a given Thue equation, but the algorithm used is of course a bit smarter, than just checking tons of integer pairs.

Bibliography

[1] E. Bombieri, W. Gubler; *Heights in Diophantine Geometry.* Cambridge University Press, 2006

[2] J. Borwein, A. van der Poorten, J. Shallit, W. Zudilin; *Neverending Fractions – An Introduction to Continued Fractions.* Cambridge University Press, 2014

[3] Y. Bugeaud; *Linear Forms in Logarithms and Applications,* IRMA Lectures in Mathematics and Theoretical Physics 28. EMS, 2018

[4] V. Dimitrov; *A Proof of the Schinzel-Zassenhaus Conjecture on Polynomials.* preprint: arXiv:1912.12545

[5] M. Hindry, J. H. Silverman; *Diophantine Geometry – An Introduction,* Graduate Texts in Mathematics 201. Springer, 2000

[6] S. Lang; *Algebra,* Graduate Texts in Mathematics 211 (3rd edition). Springer, 2002

[7] D. H. Lehmer; *Factorization of certain cyclotomic functions.* Ann. of Math. (2) 34 (1933), no. 3, 461–479

[8] D. Masser; *Auxiliary Polynomials in Number Theory.* Cambridge University Press, 2016

[9] S. Natarajan, R. Thangadurai; *Pillars of Transcendental Number Theory.* Springer, 2020

[10] J. Neukirch; *Algebraische Zahlentheorie.* Springer, 1992, (also available in an English translation)

[11] W. M. Schmidt; *Diophantine Approximation,* Lecture Notes in Mathematics 785. Springer, 1980

[12] J. H. Silverman; *The Arithmetic of Dynamical Systems,* Graduate Texts in Mathematics 241. Springer, 2007

[13] S. Ramanujan; *A Proof of Bertrand's Postulate.* J. Ind. Math. Soc.11 (1919), 181–182