DIOPHANTINE APPROXIMATIONS

LEO OUYANG

Abstract. In this mathematical paper, we will introduce Diophantine Approximations. We will explore the upper and lower bounds of Diophantine Approximations, and mainly focus on its applicability to algebraic numbers and the accuracy to which one cam approximate it using rational numbers by proving Dirichlet's Approximation Theorem, Liouville's Theorem, and Thue-Siegel-Roth's Theorem.

1. Introduction

Diophantine Approximations, named after Diophantus of Alexandria, an Alexandrian mathematician and author of *Arithmetica*, are the approximations of real numbers using rational numbers. Throughout history, there are numerous mathematicians, some of whom will be mentioned throughout this paper, whose works improved the upper and lower bounds of Diophantine Approximations.

Section 2 explores the upper bound of Diophantine Approximations and proves Dirichlet's Approximation Theorem. Section 3 focuses on the lower bound of Diophantine Approximations and proves Liouville's Theorem. Sections $4-8$ contain theorems that will be used in the proof of Thue-Siegel-Roth's Theorem. Section 4 discusses and proves theorems regarding Polynomials. Section 5 introduces and proves theorems regarding Wronskians. Section 6 considers and proves theorems regarding the indices of polynomials. Section 7 proves a combinatorical lemma. Section 8 proves the theorem that is referenced in Thue-Siegel-Roth's theorem. In Section 9, the proof of Thue-Siegel-Roth's Theorem will be given.

2. Upper Bound of Diophantine Approximations

Definition 2.1. We say $\alpha \in \mathbb{C}$ is an algebraic number if it is a root of a polynomial with a finite degree and integer coefficients.

Theorem 2.2 (Dirichlet's Approximation Theorem)**.** *Let α be an irrational number. There exists a fraction p/q, where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$, such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{2.1}$$

Proof. Let $n \geq 1$ be an integer. Let $\{x\}$ be the fractional part of x. Consider the $n+1$ fractional parts of $\{0 \cdot \alpha\}, \{1 \cdot \alpha\}, \ldots, \{n \cdot \alpha\}$, which are all within the interval of $[0, 1)$. The interval $[0, 1)$ can be split into n sub-intervals:

$$\left[0, \frac{1}{n}\right), \left[\frac{1}{n}, \frac{2}{n}\right), \ldots \left[\frac{n-1}{n}, 1\right).$$

Since there are $n+1$ fractional parts and n sub-intervals, by the Pigeonhole Principle, it implies that there exist two integers $0 \leq j < k \leq n$ such that $\{j \cdot \alpha\}$ and $\{k \cdot \alpha\}$ belong in the same sub-interval. Thus, there exists some integer p that satisfies:

$$|(k-j)\alpha - p| < \frac{1}{n}.$$

Setting $q = k - j$ and dividing by q on both sides, we get

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

□

Corollary 2.3. *There are an infinitely many irreducible fractions p/q such that*

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

Proof. According to Dirichlet's Approximation Theorem, for any irrational α, any N, there exists p, q integers $1 \leq q \leq N$ such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Nq}.$$

Since α is irrational, you can take the sequence N_N going to infinity such that

$$|q_n\alpha - p_n| < \frac{1}{N_n}.$$

Thus, the sequence q_n also has to go to infinity in order for $|q_n\alpha - p_n|$ to approach 0. If q_n is bounded, then you will always have finite values of $|q_n\alpha - p_n|$, regardless of whether p_n is bounded or not. Since α is irrational, it means $|q_n\alpha - p_n| \neq 0$ can never approach 0. Thus, it is important that q_n goes to infinity, resulting in an infinite number of solutions. □

This was the first major result that was achieved for the upper bound of Diophantine Approximations. Later on, another mathematician by the name of Adolf Hurwitz was able to strengthen this theorem with a constant.

Theorem 2.4 (Hurwitz's Theorem)**.** *Let A be a constant satisfying $0 < A \leq \sqrt{5}$. If α is irrational, then there are infinitely many rational numbers p/q satisfying*

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

The proof of this theorem can be found in [Hur91]. The constant in this theorem cannot be further improved without excluding some irrational numbers.

3. Lower Bound of Diophantine Approximations

We will now move to the lower bound. In the 1840's, Liouville obtained the first lower bound for Diophantine Approximations.

Theorem 3.1 (Liouville's Approximation Theorem)**.** *If α is an irrational algebraic number of degree $n > 1$, there exists a constant $c(\alpha)$ such that*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^n}$$

for all rationals $\frac{p}{q}$, where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. x

Proof. Let $f(z) = a_0 + a_1 z + \cdots + a_n z^n$ be the minimal polynomial, a polynomial with integer coefficients of smallest degree, having α as a root.

Let

$$M = \sup_{|z-\alpha|<1} |f'(z)|. \tag{3.1}$$

Then let p/q be a rational number such that $\left|\frac{p}{q} - \alpha\right| < 1$. By the Mean Value Theorem,

$$\left|f\left(\frac{p}{q}\right) - f(\alpha)\right| = f'(c)\left|\frac{p}{q} - \alpha\right| \leq M\left|\frac{p}{q} - \alpha\right|$$

where c is a real number that lies between α and p/q.

Since $f(z)$ does not have any rational roots,

$$0 \neq f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n + \cdots + a_0 = \frac{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n}{q^n}.$$

Since $a_0 q^n$ is a nonzero integer, the numerator has an absolute value of at least 1. Thus:

$$\left|f\left(\frac{p}{q}\right) - f(\alpha)\right| = \left|f\left(\frac{p}{q}\right)\right| = \frac{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n}{q^n} \geq \frac{1}{q^n}. \tag{3.2}$$

Combining (3.1) and (3.2), we get:

$$\frac{1}{q^n} \leq M\left|\alpha - \frac{p}{q}\right| \implies \frac{1}{Mq^n} \leq \left|\alpha - \frac{p}{q}\right|.$$

Writing $c^{-1}(\alpha)$ as M, we achieve:

$$\frac{c(\alpha)}{q^n} \leq \left|\alpha - \frac{p}{q}\right|.$$

□

This result allowed Liouville to discover the first proven example of a transcendental number, the Liouville constant.

$$\sum_{i=0}^{\infty} 10^{-i!} = 0.11000100000000000000000001000\ldots.$$

More can be found on [Lio44].

According to Liouville, there is an obvious limit to the accuracy with which algebraic numbers can be approximated by rational numbers.

Say α is an irrational algebraic number of degree $n \geq 2$. Then there are infinitely many rational numbers p/q that satisfy the inequality

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

Thue, Siegel, and Dyson would be some of the mathematicians that improved the value of κ and the accuracy of Liouville's Theorem.

Theorem 3.2 (Thue's Theorem, 1908)**.**

$$\kappa \leq \frac{1}{2}n + 1.$$

Theorem 3.3 (Siegel's Theorem, 1921)**.**

$$\kappa \leq s + \frac{n}{s+1} \text{ for } s = 1, 2, \ldots, n-1.$$

Theorem 3.4 (Dyson's Theorem, 1947)**.**

$$\kappa \leq \sqrt{2n}.$$

In 1955, Roth would prove Siegel's conjecture.

Theorem 3.5 (Roth's Theorem, 1955)**.**

$$\kappa \leq 2.$$

All of this would finally lead to the Thue-Siegel-Roth's theorem.

Theorem 3.6 (Thue-Siegel-Roth's Theorem)**.** *There exists a positive constant $c(\alpha, \epsilon)$ such that*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha, \epsilon)}{q^{2+\epsilon}}$$

holds for every rational number p/q.

In this paper, we will prove the Thue-Siegel-Roth's Theorem. This proof will be similar to LeVeque's in [LeV56, Chapter 4].

4. Polynomials

Let $P(z) = a_0 + a_1 z + \cdots + a_n z^n$ be a polynomial with complex coefficients. We start with some definitions.

Definition 4.1. Let P be the polynomial above. Then $||P|| = \max\{|a_0|, |a_1|, \ldots, |a_n|\}$. Furthermore, if α is algebraic over $\mathbb{Q}$ with its minimal polynomial $f(z)$ over $\mathbb{Q}$, we define the *height* $H(\alpha) = ||f||$.

Theorem 4.2. *Let*

$$L(z) = l \prod_{k=1}^{h} (z - \lambda_k)$$

where $l, \lambda_k \in \mathbb{C}$ *for* $k = 1, \ldots, h$. *Then*

$$|l| \prod_{k=1}^{h} (1 + |\lambda_k|) \leq 6^h \, ||L|| \,. \tag{4.1}$$

Proof. It is obvious that l can be excluded. Then, we can arrange the complex number $\lambda_1, \ldots, \lambda_h$ in such a way that $|\lambda_i| \leq 2$ for $i = 1, \ldots, t$ and $|\lambda_i| > 2$ for $i > t$. Say z_0 is the $(t+1)$th root of unity. For each $k = t+1, \ldots, h$, we can divide $1 + |\lambda_k|$ with $|z_0 - \lambda_k|$, achieving:

$$\frac{1 + |\lambda_k|}{|z_0 - \lambda_k|} \leq \frac{1 + |\lambda_k|}{|\lambda_k| - |z_0|} = \frac{1 + |\lambda_k|}{|\lambda_k| - 1} = 1 + \frac{2}{|\lambda_k| - 1} < 1 + \frac{2}{2 - 1} = 3.$$

Thus,

$$\prod_{k=t+1}^{h} (1 + |\lambda_k|) < 3^{h-t} \left| \prod_{k=t+1}^{h} (z_0 - \lambda_k) \right|. \tag{4.2}$$

For the remaining $k = 1, 2, \ldots, t$ we can say

$$\prod_{k=1}^{t} (1 + |\lambda_k|) \leq (1 + 2)^t = 3^t.$$

Assuming that $|f(z_0)| \geq 1$, where $f(z) = \prod_{k=1}^{t} (z - \lambda_k)$ and z_0 is the previous $(t+1)$th root of unity, we obtain

$$\prod_{k=1}^{t} (1 + |\lambda_k|) \leq 3^t \leq 3^t \left| \prod_{k=1}^{t} (z_0 - \lambda_k) \right|.$$

Combining this with (4.2), we get

$$\prod_{k=1}^{h} (1 + |\lambda_k|) < 3^h \left| \prod_{k=1}^{h} (z_0 - \lambda_k) \right|$$

.

Since $f(z_0) \leq ||L|| \left(|z_0|^h + \cdots + 1\right)$,

$$3^h \left| \prod_{k=1}^{h} (z_0 - \lambda_k) \right| \leq 3^h \, ||L|| \left(|z_0|^h + \cdots + 1\right) = 3^h \, ||L|| \, (h+1) \leq 6^h \, ||L|| \, .$$

To prove that $|f(z_0)| \geq 1$ does exist, we first let ϵ be the $(t+1)$th root of unity. Set

$$f(z) = \sum_{r=0}^{t} \mu_r z^r, \quad \mu_t = 1.$$

Then

$$\sum_{v=0}^{t} \epsilon^v f(\epsilon^v) = \sum_{v=0}^{t} \left(\epsilon^v \sum_{r=0}^{t} \mu_r \epsilon^{vr} \right) = \sum_{r=0}^{t} \left(\mu_r \sum_{v=0}^{t} \epsilon^{v(r+1)} \right).$$

Focusing on $\sum_{v=0}^{t} \epsilon^{v(r+1)}$, if $(t+1) \mid (r+1)$ this sum clearly equals $t+1$. Since $0 \leq r \leq t$ this is only true when $r = t$. If $(t+1) \nmid (r+1)$, then the sum reduces to

$$\sum_{v=0}^{t} z^v = \frac{z^{n+1} - 1}{z - 1} = 0.$$

Thus,

$$\sum_{v=0}^{t} \epsilon^v f(\epsilon^v) = \mu_t (t+1) = t+1.$$

Hence

$$\sum_{v=0}^{t} |f(\epsilon^v)| = \sum_{v=0}^{t} |\epsilon^v f(\epsilon^v)| \geq \left| \sum_{v=0}^{t} \epsilon^v f(\epsilon^v) \right| = t+1.$$

Therefore, there exists a root of unity $z_0 \in \{1, \epsilon, \epsilon^2, \ldots, \epsilon^t\}$ such that $|f(z_0)| \geq 1$.

□

Now we move to some more theorems that will be useful later on.

Theorem 4.3. *Let $f(z)$ and $g(z)$ be complex polynomials of degree n and m respectively. Suppose the coefficient of z^m in $g(z)$ has an absolute value greater than or equal to 1. Then*

$$||f|| \leq 6^{m+n} \, ||fg||$$

Proof. Let

$$\begin{aligned} f(z) &= a_0 \, (z - \lambda_1) \cdots (z - \lambda_n) \\ g(z) &= b_0 \, (z - \lambda_{n+1}) \cdots (z - \lambda_{n+m}) \, . \end{aligned}$$

Then

$$\begin{aligned} ||f|| &\leq \left|\left| a_0 \prod_{k=1}^{n} (z + |\lambda_k|) \right|\right| \leq |a_0 b_0| \cdot \prod_{k=1}^{n} (1 + |\lambda_k|) \\ &\leq |a_0 b_0| \cdot \prod_{k=1}^{n} (1 + |\lambda_k|) \, , \end{aligned}$$

and we get our desired result using Theorem 4.2.

□

Theorem 4.4. *Let $f(z)$ be polynomial of degree n, having real coefficients. Then*

$$||f||^m \leq (mn + 1) \, ||f^m||$$

See [LeV56, Theorem 4-4] for the full proof.

We now turn to some definitions.

Definition 4.5. Let α is an algebraic number of degree n, with corresponding minimal polynomial $p(z)$. Then the roots, $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$, of $p(z)$ are called the conjugates of α.

Definition 4.6. Let $P(z)$ be a polynomial with algebraic coefficients $c_1, c_2, \ldots, c_r$. Also let C_i equal the maximum of the absolute values of the conjugates of c_i. Then we define $\left|\overline{P}\right|$ as $\left|\overline{P}\right| = \max\{C_1, C_2, \ldots, C_r\}$. If α is algebraic we also define $|\overline{\alpha}|$ as the maximum of the absolute values of the conjugates of α.

Theorem 4.7. *If $f_1(z), f_2(z), \ldots, f_t(z)$ are polynomials with algebraic coefficients, then*

$$\left|\overline{\prod_{v=1}^{t} f_v}\right| \leq \prod_{v=1}^{t} (1 + \deg f_v) \prod_{v=1}^{t} \left|\overline{f_v}\right|.$$

Proof. Suppose, without loss in generality, that $\deg f_1 \geq \deg f_2 \geq \cdots \geq \deg f_t$.

Each coefficient of $f_1 f_2$ will be a polynomial the sum of products of a coefficient f_1 and a coefficient of f_2. The number of sums of products will be at most $\operatorname{def} f_2 + 1$, so we achieve:

$$\left|\overline{f_1 f_2}\right| \leq (\deg f_2 + 1) \left|\overline{f_1}\right| \left|\overline{f_2}\right|.$$

Then we can also say that

$$\left|\overline{f_1 f_2 f_3}\right| \leq (1 + \deg) f_3 \left|\overline{f_1 f_2}\right| \left|\overline{f_3}\right| \leq (1 + \deg)(1 + \deg f_2) \left|\overline{f_1}\right| \left|\overline{f_2}\right| \left|\overline{f_3}\right|,$$

and so on.

□

Theorem 4.8. *Let p and r be positive integers with $1 \leq r < p$. Suppose that $F(z_1, \ldots, z_p)$, $G(z_1, \ldots, z_r)$, and $H(z_{r+1}, \ldots, z_p)$ are polynomials with coefficients in an algebraic number field K, those of F being integers. Also suppose that*

$$F(z_1, \ldots, z_p) = G(z_1, \ldots, z_r) H(z_{r+1}, \ldots, z_p).$$

Then if γ is any coefficient in F, there is a factorization $\gamma = \alpha\beta$ in K such that the coefficients in αH and βG are integers in K.

Proof. Let the coefficients in G be $\alpha_1, \ldots, \alpha_s$, and those in H be $\beta_1, \ldots, \beta_t$, in some order. Since the variables in G and H are disjoint, that means that the variables in F are simply the products $\alpha_i \beta_j$. Since the coefficients in F are integers, the products $\alpha_i \beta_1, \ldots, \alpha_i \beta_t$ and $\beta_j \alpha_1, \ldots, \beta_j \alpha_s$ are also integers. But these two sets of numbers are just the coefficients in $\alpha_1 H$ and $\beta_1 G$.

□

5. Generalized Wronskians

Now we turn our attention to Wronskians. The results from this section will be needed in the next one.

Throughout this section $f_0(z_1,\dots,z_p),\dots,f_{l-1}(z_1,\dots,z_p)$ are polynomials in an algebraic number field K.

Definition 5.1. $f_0,\dots,f_{t-1}$ are said to be linearly dependent if

$$k_0f_0+\cdots+k_{l-1}f_{l-1}=0,\ k_i\in K \text{ for each } i=0,\dots,l-1,$$

if there exists some linear combination, where the constant coefficients are not all zero, vanishes identically. Otherwise, $k_0,\dots,k_{l-1}$ are said to be linearly independent.

If $p=1$, then we define the Wronskian as

$$\begin{aligned}W(z)&=\begin{vmatrix}\frac{1}{0!}f_0(z) & \frac{1}{0!}f_1(z) & \cdots & \frac{1}{0!}f_{l-1}(z)\\ \frac{1}{1!}f_0'(z) & \frac{1}{1!}f_1'(z) & \cdots & \frac{1}{1!}f_{l-1}'(z)\\ \vdots & \vdots & \ddots & \vdots\\ \frac{1}{(l-1)!}f_0^{(l-1)}(z) & \frac{1}{(l-1)!}f_1^{(l-1)}(z) & \cdots & \frac{1}{(l-1)!}f_{l-1}^{(l-1)}(z)\end{vmatrix}\\ &=\det\left(\frac{1}{\mu!}\frac{d^\mu}{dz^\mu}f_v(z)\right),\ \mu,\ v=0,1,\dots,l-1.\end{aligned}$$

For convenience's sake, we include the factors $\frac{1}{\mu!}$, $\mu=0,\dots,l-1$.

The Generalized Wronskian deals with all the cases $p\geq 1$. Let $\Delta_0,\dots,\Delta_{l-1}$ be differential operators of the form

$$\Delta_\mu=\frac{1}{j_1!\cdots j_p!}\left(\frac{\partial}{\partial z_1}\right)^{j_1}\cdots\left(\frac{\partial}{\partial z_p}\right)^{j_p}$$

such that the order $j_1+\cdots j_p$, of Δ_μ does not exceed μ for any $\mu=0,\dots,l-1$. Then we can define the generalized Wronskian as

$$G(z)=\begin{vmatrix}\Delta_0f_0(z) & \Delta_0f_1(z) & \cdots & \Delta_0f_{l-1}(z)\\ \Delta_1f_0(z) & \Delta_1f_1(z) & \cdots & \Delta_1f_{l-1}(z)\\ \vdots & \vdots & \ddots & \vdots\\ \Delta_{l-1}f_0(z) & \Delta_{l-1}f_1(z) & \cdots & \Delta_{l-1}f_{l-1}(z)\end{vmatrix}.$$

Since there are several different Δ_μ's for each μ, there is not just one generalized Wronskian. The number of different Δ_μ's are $(p+1)^\mu$.

We now turn to two theorems that will be needed later. Due to the length of their proofs, they will not be included in this paper. For full proofs see [LeV56, Chapter 4].

Theorem 5.2. *(a) If $f_0, \ldots, f_{l-1}$ are l polynomials over K in the single variable z, whose Wronskian $W(z)$ vanishes identically, then they are dependent of K.*

(b) If $f_0, \ldots, f_{l-1}$ are l polynomials over K in the variables $z_1, \ldots, z_p$, for which every generalized Wronskian $G_l(z_1, \ldots, z_p)$ vanishes identically, then they are dependent.

Theorem 5.3. *Let $R(z_1, \ldots, z_p)$ be a polynomial in $p \geq 2$ variables, with integral coefficients in K such that*

$$0 < \left|\overline{R}\right| \leq B.$$

Let R be of degree at most r_j in z_j, for $j = 1, \ldots, p$. Then there is an l in $\mathbb{Z}$ with

$$1 \leq l \leq r_p + 1,$$

there is an integer β in K, and there are differential operators $\Delta_0, \ldots, \Delta_{l-1}$ on the variables $z_1, \ldots, z_{p-1}$ of orders at most $0, \ldots, l-1$ respectively, such that if

$$F(z_1, \ldots, z_p) = \beta det\left(\Delta_\mu \frac{1}{v!}\left(\frac{\partial}{\partial z_p}\right)^v R\right), \quad \mu, v = 0, \ldots, l-1,$$

then (a) F has integral coefficients in K and is not identically zero; (b) a decomposition

$$F(z_1, \ldots, z_p) = U(z_1, \ldots, z_{p-1})\, V(z_p)$$

holds, where U and V have integral coefficients in K, U is of degree at most lr_j in z_j for $j = 1, \ldots, p-1$, and V is of degree at most lr_p in z_p; (c) the following bounds holds:

$$\left|\overline{F}\right| \leq \{(r_1+1)\ldots(r_p+1)\}^{2l} 2^{2(r_1+\cdots+r_p)l} l!^2 B^{2l}.$$

6. The Index

In this section we will mention the theorems with indexes. Their proofs can be found in [Ish08, Section 4].

We say $P(z_1, \ldots, z_p)$ is a non-zero polynomial, while $\overline{\alpha}_p = (\alpha_1, \ldots, \alpha_p)$ and $\overline{r}_p = (r_1, \ldots, r_p)$ are lists of complex numbers and positive numbers, respectively.

Now, expand the polynomial $P(\alpha_1 + y_1, \ldots, a_p + y_p)$ in $y_1, \ldots, y_p$, i.e.,

$$P(\alpha_1 + y_1, \ldots, a_p + y_p) = \sum_{j_1=0}^{\infty} \cdots \sum_{j_p=0}^{\infty} c(j_1, \ldots, j_p) y_1^{j_1} \cdots y_p^{j_p}.$$

Definition 6.1. The index θ of P at point $\overline{\alpha}_p$* relative to $\overline{r}_p$ is

$$\theta = \min \left(\frac{j_1}{r_1} + \cdots + \frac{j_p}{r_p} \right),$$

where the minimum is extended over the set of nonnegative integers $j_1, \ldots, j_p$ for which $c(j_1, \ldots, j_p) \neq 0$.

Theorem 6.2. *Let $P(z_1, \ldots, z_p)$ and $Q(z_1, \ldots, z_p)$ be non-zero polynomials that do not vanish identically. If we consider the indices at the same point $\overline{\alpha}_p$ relative to the same list of numbers $\overline{r}_p$, then the following relations hold:*

$$index\,(P + Q) \geq \min\,(index\ P,\ index\ Q),$$

$$index\ PQ = index\ P + \ index\ Q.$$

Let K be an algebraic number field, $B \geq 1$ and consider the set $\mathcal{R}_m = \mathcal{R}_m(B; \overline{r}_m)$ of polynomials $R \in K[z_1, \ldots, z_m]$ with the properties:

(i) R is of degree at most r_j in z_j, for $j = 1, \ldots, m$,
(ii) and $\left|\overline{R}\right| \leq B$.

Let $\zeta_1, \ldots, \zeta_m$ be algebraic numbers in $\mathbb{C}$ of heights $q_1, \ldots, q_m$ respectively. Let $\theta(R)$ denote the index of $R(z_1 \ldots, z_m)$ at the points $\overline{\zeta}_m = (\zeta_1, \ldots, \zeta_m)$ relative to $\overline{r}_m$. Now we will proceed to create definations which will be useful later on.

Definition 6.3. We say

$$\Theta_m(B; \overline{q}_m; \overline{r}_m = \sup\{\theta(R)\}$$

is the supremum or the upper bound that is iterated over all $R \in \mathcal{R}_m$ and all list $\overline{\zeta}_m$ with elements of heights $q_1, \ldots, q_m$†

To find an upper bound for $\Theta_m(B; \overline{q}_m; \overline{r}_m)$, we will use induction on m and proceed with the theorem that will be used later in the case $m = 1$.

*Note that we refer to $\overline{\alpha}_p$ as a point here.

†I.e. $H(\zeta_1) = q_1, \ldots, H(\zeta_m) = q_m$.

Theorem 6.4.

$$\Theta_1\left(B;\overline{q}_1;\overline{r}_1\right) \leq \frac{3N(N+1)}{\log q1} + \frac{N\log B}{r_1\log q_1},^{\ddagger}$$

where $N = [K:\mathbb{Q}]$.

With this, we can find a recurrence relation between Θ_m and Θ_{m-1}.

Theorem 6.5. *Let* $p \geq 2$ *be a positive integer, let* $r_1, \ldots, r_p$ *be positive integers such that*

$$r_p > 10\delta^{-1}, \frac{r_{j-1}}{r_j} > \delta^{-1}, \text{ for } j = 2, \ldots, p, \tag{6.1}$$

where $0 < \delta < 1$, *let* $q_1, \ldots, q_p$ *be positive integers. Then*

$$\Theta_p(B;\overline{q}_p;\overline{r}_p) \leq 2\max(\Phi + \Phi^{\frac{1}{2}} + \delta^{\frac{1}{2}}), \tag{6.2}$$

where the maximum is taken over integers l *satisfying*

$$1 \leq l \leq r_p + 1,$$

and where

$$\Phi = \Theta_1(M;q_p;lr_p) + \Theta_{p-1}(M;\overline{q}_{p-1};\overline{lr}_{p-1})$$

and

$$M = (r_1+1)^{2pl}2^{2r_1pl}l!^2B^{2l}.$$

‡If we only consider the index of a polynomial at the point $\overline{\alpha}_p$ of real numbers, then the term $\frac{3N(N+1)}{\log q1}$ could be neglected. This was what Roth did in his original proof. See [Rot55].

Now, we use Theorem 6.4 and 6.5 for the main theorem in this section.

Theorem 6.6. *Let m be a positive integer, and suppose that*

$$0 < \delta < \frac{1}{m2^m(N+1)^2}. \tag{6.3}$$

Let $r_1, \dots, r_m$ be positive integers such that

$$r_m > 10\delta^{-1}, \frac{r_{j-1}}{r_j} > \delta^{-1}, \text{ for } j = 2, \dots, m. \tag{6.4}$$

Let $q_1, \dots, q_m$ be positive integers such that

$$\log q_1 > 2\delta^{-1}m(2m+1), \tag{6.5}$$

$$r_j \log q_j \geq r_1 \log q_1, \text{ for } j = 2, \dots, m, \tag{6.6}$$

$$\log q_1 > 3\delta^{-1}N(N+1), \tag{6.7}$$

Then

$$\Theta(q_1^{\delta r_1}; \overline{q}_m; \overline{r}_m) < 10^m \delta^{(\frac{1}{2})^m}. \tag{6.8}$$

7. A Combinatorical Lemma

In this section, we will mention the Combinatorical Lemma. Due to its length, we will not go over the proof. The proof can be found in [Ish08, Section 5].

Definition 7.1. Let $r_1, \dots, r_m$ be positive integers, and $\lambda > 0$. Let $(j_1 \dots, j_m)$ be a list of integers such that

$$0 \leq j_1 \leq r_1, \dots, 0 \leq j_m \leq r_m \tag{7.1}$$

and

$$\frac{j_1}{r_1} + \cdots + \frac{j_m}{r_m} \leq \frac{1}{2}(m - \lambda). \tag{7.2}$$

If A is the set of all such lists of integers, then $A_m(\lambda)$ is defined as

$$A_m(\lambda) = |A|$$

Theorem 7.2. *If ${}_r1, \dots, r_m$ and λ are as in the above definition, then*

$$A_m(\lambda) \leq 2\sqrt{m}\lambda^{-1}(r_1+1)\cdots(r_m+1). \tag{7.3}$$

8. The Approximation Polynomial

In this section, we will prove the theorem which is the only one referenced in the proof of the Thue-Siegel-Roth theorem.

Let α be an algebraic integer of degree $n \geq 2$ over K. Let $\omega_1, \ldots, \omega_N$ be an integral basis for K, and put

$$|\overline{\alpha}| = b_1 \geq 1, \ \max\left(|\overline{\omega_1}|, \ldots, |\overline{\omega_N}|\right) = b_2.$$

That $\omega_1, \ldots, \omega_N$ is an integral basis for K mean that every element $\mathcal{O}_K$ can be written uniquely as a linear combination of $\{\omega_1, \ldots, \omega_N\}$ with coefficients in $\mathbb{Z}$.

We will later choose the variables $m, \delta, q_1, \zeta_1, \ldots, q_m, \zeta_m, r_1, \ldots, r_m$, in the given order just specified, such that they satisfy the following conditions:

$$0 < \delta < \frac{1}{m2^m(N+1)^2}, \tag{8.1}$$

$$10^m \delta^{(\frac{1}{2})^m} + 2(1+3\delta)n\sqrt{m} < \frac{m}{2}, \tag{8.2}$$

$$r_m > 10\delta^{-1}, \frac{r_{j-1}}{r_j} > \delta^{-1}, \text{ for } j = 2, \ldots, m, \tag{8.3}$$

$$\delta^2 \log q_1 > 2m + 1 + m\log(b_1 + 1) + 4b_2 N, \tag{8.4}$$

$$r_j \log q_j \geq r_1 \log q_1, \text{ for } j = 2, \ldots, m, \tag{8.5}$$

$$\log q_1 > 3\delta^{-1} N(N+1). \tag{8.6}$$

Below are some variables that are defined to simplify later calculations:

$$\lambda = 4(1+3\delta)n\sqrt{m}, \tag{8.7}$$

$$\mu = \frac{1}{2}(m - \lambda), \tag{8.8}$$

$$\eta = 10^m \delta^{(\frac{1}{2})^m}, \tag{8.9}$$

$$B_1 = \lfloor q_1^{\delta r_1} \rfloor. \tag{8.10}$$

Theorem 8.1. *Suppose that the conditions (8.1) - (8.6) are satisfied, and suppose that $\delta_1, \dots, \delta_m$ are algebraic numbers of heights $q_1, \dots, q_m$, respectively. Then there exists a polynomial $Q \in K[z_1, \dots, z_m]$ with integral coefficients in K and of degree at most r_j in z_j, for $j = 1, \dots, m$, such that*

(i) *the index of Q at the point $(\alpha, \dots, \alpha)$ relative to $r_1, \dots, r_m$ is at least $\mu - \eta$;*
(ii) *$Q(\zeta_1, \dots, \zeta_m) \neq 0$;*
(iii) *for all derivatives*

$$Q_{i_m \dots i_m}(z_i, \dots, z_m) = \frac{1}{i_1! \cdots i_m!} \left(\frac{\partial}{\partial z_1}\right)^{i_1} \cdots \left(\frac{\partial}{\partial z_m}\right)^{i_m} Q,$$

where $i_m \dots i_m$ are non-negative integers, the inequality

$$|Q_{i_m \dots i_m}(z_i, \dots, z_m)| < B_1^{1+3\delta}(1 + |z_1|)^{r_1} \cdots (1 + |z_m|)^{r_m}$$

holds, and the corresponding inequality also holds if the coefficients in Q are replaced by their respective field conjugates.

Proof. Let C be the set of integers of K of the form

$$c_1\omega_1 + \cdots + c_N\omega_N,$$

where $c_1, \dots, c_N$ range over all non-negative integers not exceeding B_1. If we put

$$(1 + r_1) \cdots (1 + r_m) = r,$$

then there are $|C|^r = (1 + B_1)^{Nr}$ distinct polynomials

$$P(z_1, \dots, z_m) = \sum_{s_1=0}^{r_1} \cdots \sum_{s_m}^{r_m} \gamma(s_1, \dots, s_m) z_1^{s_1} \cdots z_m^{s_m}$$

whose coefficients $\gamma(s_1, \dots, s_m) \in C$. If we put

$$\begin{aligned} P_{i_1 \dots i_m}(z_1, \dots, z_m) &= \frac{1}{i_1! \cdots i_m!} \left(\frac{\partial}{\partial z_1}\right)^{i_1} \cdots \left(\frac{\partial}{\partial z_m}\right)^{i_m} P(z_1, \dots, z_m) \\ &= \sum_{s_1=0}^{r_1} \cdots \sum_{s_m=0}^{r_m} \gamma(s_1, \dots, s_m) \binom{r_1}{j_1} \cdots \binom{r_m}{j_m} z_1^{s_1 - j_1} \cdots z_m^{s_m - j_m}, \end{aligned}$$

then

$$\left|\overline{P_{j_1,\dots j_m}}\right| \le 2^{r_1+\cdots+r_m} b_2 B_1 N \le b_2 N 2^{mr_1} B_1 < b_2 N B_1^{1+\delta},$$

since

$$\left|\overline{\gamma(s_1,\dots s_m)}\right| \le b_2 B_1 N, \tag{8.11}$$

$$mr_1 \log 2 < r_1[m(1+\log\sqrt{b_1+1}] < \frac{1}{2} r_1[2m + 1m\log(b_1+1) + 4b_2 N] < \frac{1}{2}\delta^2 r_1 \log q_1,$$

$$\binom{r_k}{j_k} < 2^{r_k}$$

and $q_1^{\frac{1}{2}r_1} < B_1$. Also, since, by (8.4),

$$r \le 2^{r_1+\cdots+r_m} \le 2^{mr_1} \le (b_1+1)^{mr_1} < B_1^{\delta},$$

we obtain the bound

$$\begin{aligned}\left|\overline{P_{j_1,\dots j_m}(\alpha,\dots,\alpha)}\right| &\le b_2 N B_1^{1+\delta} r b_1^{r_1+\cdots+r_m} \\ &\le b_2 N B_1^{1+3\delta}.\end{aligned} \tag{8.12}$$

Let ϑ be a primitive element of L, so that $L = \mathbb{Q}(\vartheta)$. Order the conjugates of ϑ so that $\vartheta_1,\dots,\vartheta_{p_1}$ are real and $\overline{\vartheta_{p_1+v}} = \overline{\vartheta_{p_1+p_2+v}}$ are complex conjugates for $v = 1,\dots,p_2$, $P_{j_1\dots j_m}(\alpha,\dots,\alpha)$, where $j_1,\dots,j_m$ satisfy the given inequalities

$$0 \le j_1 \le r_1,\dots,0 \le j_m \le r_m, \quad \frac{j_1}{r_1} + \cdots + \frac{j_m}{r_m} \le \mu. \tag{8.13}$$

Then ξ can be written as a polynomial in ϑ, with rational coefficients, with the field conjugates $\xi^{(v)}$, for $v = 1,\dots,nN$, i.e., if

$$\xi = a_0 + a_1\vartheta^1 + \cdots + a_{n-1}\vartheta^{nN-1},$$

where $a_i \in \mathbb{Q}$, for $i = 1,\dots,nN$, then

$$\xi^{(v)} = a_0 + a_1\vartheta_v^1 + \cdots + a_{n-1}\vartheta_v^{nN-1},$$

is a field conjugate, where ϑ_v is one of the conjugates of ϑ. We can define nN real numbers $\xi_1,\dots,\xi_{nN}$ by the equations

$$\begin{aligned}\xi_v &= \xi^{(v)}, \quad \text{for } v = 1,\dots,p_1, \\ \xi_v + i\xi_{v+p_2} &= \xi^{(v)}, \quad \text{for } v = p_1+1,\dots,p_1+p_2.\end{aligned}$$

Fixing the coefficients $\gamma(s_1, \dots, s_m)$, we can then arrange the ξ_v's in a fixed order and each of these numbers can be viewed as coordinates of a point. Doing this for all $j_1, \dots, j_m$ satisfying (8.13), we get, by Theorem 7.2,

$$M \leq 2nN\sqrt{m}\lambda^{-1}r$$

coordinates. Furthermore, from (8.12) we see that each of the coordinates have absolute values smaller than $\lfloor b_2 N B_1^{1+3\delta} \rfloor + 1 = t$. Thus all points for various $\gamma(s_1, \dots, s_m) \in C$ lie in a cube of edge $2t$ in M-dimensional space. We can divide the cube into $(3t)^M$ subcubes of edge $\frac{2}{3}$. If

$$|C|^r = (1 + B_1)^{Nr} > (3t)^M, \tag{8.14}$$

then there exists more points than subcubes and thus the points corresponding to two different polynomials $P^*(z_1, \dots, z_m)$ and $P^{**}(z_1, \dots, z_m)$ lie in the same subcube. If we put

$$\overline{P} = P^* - P^{**},$$

then the point $\overline{P}_{j_1,\dots,j_m}(\alpha, \dots, \alpha)$ is in one of the 2^M subcubes closest to the origin, thus

$$\left|\overline{\overline{P}_{j_1,\dots,j_m}(\alpha, \dots, \alpha)}\right| \leq \sqrt{2} \times \frac{2}{3} < 1,$$

for all $j_1, \dots, j_m$ satisfying (8.13). But, since $\overline{P}_{j_1,\dots,j_m}(\alpha, \dots, \alpha)$ is an algebraic integer, this can only be true if it equals zero. Since this is true for all $j_1, \dots, j_m$ satisfying (8.13), the index of $\overline{P}$ at $(\alpha, \dots, \alpha)$ relative to $r_1, \dots, r_m$ must be greater than μ. The coefficients of $\overline{P}$ are the differences of two elements of C, and thus it is not hard to see that the inequality (8.11) holds for them.

We now verify that (8.14) indeed holds, so that the above conclusions are valid. Notice that by (8.4)

$$q_1^{\delta r_1} > 4b_2 N,$$

so

$$\begin{aligned} B_1 &> 4b_2 N, \\ B_1^{Nr} &> (4b_2 N B_1)^{\frac{1}{2}Nr}, \\ B_1^{Nr} &> (3b_2 N B_1^{1+3\delta} + 3)^{\frac{1}{2}Nr(1+3\delta)^{-1}}, \\ (1 + B_1)^{Nr} &> (3t)^M, \end{aligned}$$

where the third inequality follows from the fact that $B_1 > e^{15} > 3$.

Now, $\overline{P} \in \mathcal{R}_m(q_1^{\delta r_1}; \overline{r_m})$, its index at $(\zeta_1, \ldots, \zeta_m)$ relative to $r_1, \ldots, r_m$ must be less than η, by Theorem 6.5. Hence there exists a different operator

$$\Delta_k = \frac{1}{k_1! \cdots k_m!} \left(\frac{\partial}{\partial z_1}\right)^{k_1} \cdots \left(\frac{\partial}{\partial z_m}\right)^{k_m}$$

with

$$Q(z_1, \ldots, z_m) = \Delta_k \overline{P},$$

so that if

$$\frac{k_1}{r_1} + \cdots + \frac{k_m}{r_m} < \eta,$$

then

$$Q(\zeta_1, \ldots, \zeta_m) \neq 0.$$

The index of Q at the point $(\alpha, \ldots, \alpha)$ relative to $r_1, \ldots, r_m$ is at least $\mu - \eta$. Notice that by (8.2) $\mu - \eta$. Thus (i) and (ii) are satisfied.

From (8.11) and the inequality $r < B_1^{\delta}$,

$$\left|\overline{Q}\right| \leq 2^{r_1 + \cdots + r_m} b_2 N B_1 < 2^{m r_1} b_2 N B_1 < b_2 N B_1^{1+\delta},$$

and hence

$$\left|\overline{Q_{i_1, \ldots i_m}}\right| < 2^{r_1 + \cdots + r_m} b_2 N B_1^{1+\delta} < b_2 N B_1^{1+2\delta}.$$

Finally,

$$\begin{aligned} |Q_{i_1, \ldots i_m}(z_1, \ldots z_m)| &< b_2 N B_1^{1+2\delta} \prod_{v=1}^{m} (1 + |z_v| + \cdots + |z_v|^{r_v}) \\ &< b_2 N B_1^{1+2\delta} \prod_{v=1}^{m} (1 + |z_v|)^{r_v} \\ &< B_1^{1+3\delta} \prod_{v=1}^{m} (1 + |z_v|)^{r_v}, \end{aligned}$$

where the last inequality follows since $b_2 N < B_1^{\delta}$ by (8.4). The same inequality holds if the coefficients are replaced by their respective field conjugates, and thus we are done.

□

9. Proof of the Thue-Siegel-Roth's Theorem

Theorem 9.1 (Generalization of the Thue-Siegel-Roth's theorem)**.** *Let K be an algebraic number field of degree N, i.e., $[K:\mathbb{Q}]=N$, and let α be algebraic of degree $n\geq 2$ over K. Then for each $\kappa>2$, the inequality*

$$|\alpha-\zeta|<\frac{1}{[H(\zeta)]^{\kappa}} \tag{9.1}$$

has only finitely many solutions for ζ in K.

Proof. We will prove this theorem by assuming it is false and achieving a contradiction.

Let the monic defining polynomial of α be $p(z)=z^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0$ Furthermore, let a equal the least common multiple of the denominators of the rational coefficients of $p(z)$. Then $q(z)=a^np\left(\frac{z}{a}\right)$ has integral coefficients, is monic and irreducible. $a\alpha$ is a root of the equation, implying $a\alpha$ is an algebraic integer. Suppose ζ is a solution of (9.1). Then

$$|a\alpha-a\zeta|<\frac{\alpha}{[H(\zeta)]^{\kappa}}\leq\frac{a^{\kappa N+1}}{[H(a\zeta)]^{\kappa}},$$

where the last inequality follows from the fact that ζ, and viz. $a\zeta$, can be at most of degree N, thus $H(a\zeta)\leq a^NH(\zeta)$. Hence, for arbitrary $\epsilon>0$, and for all solutions ζ with $H(\zeta)$ sufficiently large,

$$|a\alpha-a\zeta|<\frac{1}{[H(a\zeta)]^{\kappa-\epsilon}},$$

and ϵ can be chosen so small that $\kappa-\epsilon>2$. Thus we can assume that α is an algebraic integer. We also realize that can ignore the ζ's for which $H(\zeta))$ is not sufficiently large since K is an algebraic number field, and thus a finite extension, resulting in only a finite amount of cases. We also note that we only need to prove the theorem for primitive elements ζ in K. This is because the number of subfields of an algebraic number field is finite and each element of K is a primitive element in such a subfield, thus the proof can be repeated. Choose m to be a rational integer so that $m>4n\sqrt{m}$ and

$$\frac{2m}{m-4n\sqrt{m}}<\kappa. \tag{9.2}$$

By first inequality, the right-hand side of (9.2) is positive and $\frac{2m}{m-4n\sqrt{m}}\to 2$ as $m\to\infty$. Thus, there exists an m since κ is strictly greater than 2. Furthermore, for sufficiently small δ, we have

$$m-4(1+3\delta)n\sqrt{m}-2\eta>0,$$

where η was defined in (8.9). This inequality is the same as the one in (8.2). We choose δ to satisfy this, (8.1) and the inequality

$$\frac{2m(1+\delta)+2\delta N(2+5\delta)}{m-4(1+3\delta)n\sqrt{m}-2\eta}<\kappa \tag{9.3}$$

which is possible because of (9.2). Using (8.7) and (8.8), we can write this inequality as

$$\frac{m(1+\delta)+\delta N(2+5\delta)}{\mu-\eta}<\kappa. \tag{9.4}$$

We now choose a primitive solution ζ_1 of (9.1) such that $q_1 = H(\zeta_1)$ satisfies (8.4) and (8.6).Then, we choose further primitive solutions $\zeta_2,\dots,\zeta_m$ of heights $q_2,\dots,q_m$, respectively, such that for $j=2,\dots,m$,

$$\frac{\log q_j}{\log q_{j-1}}>\frac{2}{\delta}. \tag{9.5}$$

We now let r_1 be any rational integer such that

$$r_1>\frac{10\log q_m}{\delta\log q_1}, \tag{9.6}$$

and define r_j, for $j=2,\dots,m$, by

$$\frac{r_1\log q_1}{\log q_j}\le r_j<\frac{r_1\log q_1}{\log q_j}+1. \tag{9.7}$$

This satisfies (8.5). Notice it gives us

$$\frac{r_j\log q_j}{r_1\log q_1}<1+\frac{\log q_j}{r_1\log q_1}<1+\frac{\log q_m}{r_1\log q_1}<1+\frac{\delta}{10}, \tag{9.8}$$

where (9.5) is used for the second inequality and (9.6) for the third. The conditions (8.3) are satisfied since

$$r_m\ge\frac{r_1\log q_1}{\log q_m}>10\delta^{-1},$$

by (9.7) and (9.6), and

$$\begin{aligned}\frac{r_{j-1}}{r_j}&>\left(\frac{\log q_j}{r_1\log q_1+\log q_j}\right)\left(\frac{r_1\log q_1}{\log q_{j-1}}\right)=\frac{\log q_j}{\log q_{j-1}}\left(\frac{r_1\log q_1}{r_1\log q_1+\log q_j}\right)\\&=\frac{\log q_j}{\log q_{j-1}}\left(1+\frac{\log q_j}{r_1\log q_1}\right)^{-1}>\frac{\log q_j}{\log q_{j-1}}\left(1+\frac{\delta^{-1}}{10}\right)^{-1}\\&>\frac{2}{\delta}\left(1+\frac{\delta^{-1}}{10}\right)^{-1}>\frac{2}{\delta}>\delta^{-1}.\end{aligned}$$

Let $Q(z_1,\dots,z_m)$ be the polynomial as in Theorem 8.1. Let $\zeta_1,\dots,\zeta_m\in K$ be zeros of irreducible polynomials of degree N with relatively prime coefficients in $\mathbb{Z}$, and the coefficients in z^N being $k_1,\dots,k_m$, respectively. Then the number

$$\phi=Q(\zeta_1,\dots,\zeta_m)$$

is in K. If the field conjugates of ζ_i are $\zeta_i',\zeta_i'',\dots$, for $i=1,\dots,m$, then $\mathrm{No}_{K/\mathbb{Q}}(\phi)$ is a sum of products of powers of the $\zeta_i^{(j)}$ with integral coefficients from K. In each such product, the factor $\zeta_i^{(j)}$ occurs to the power r_i at most. It can be shown that the product of k_i and any

set of distinct conjugates of $\zeta_i^{(j)}$ is an algebraic integer. For each i, the field conjugates of ζ_i are distinct, because ζ_i is a primitive element of K. It follows that $k_1^{r_1}\cdots k_m^{r_m}\mathrm{No}_{K/\mathbb{Q}}(\phi)$ is an algebraic integer, and since it is also rational it is a rational integer, hence

$$\left|k_1^{r_1}\cdots k_m^{r_m}\mathrm{No}_{K/\mathbb{Q}}(\phi)\right| \geq 1. \tag{9.9}$$

From (i) in Theorem 8.1. we have that the terms in

$$Q(\zeta_1,\ldots,\zeta_m)=\sum_{i_1=0}^{r_1}\cdots\sum_{i_m=0}^{r_m}Q_{i_1,\ldots,i_m}(\alpha,\ldots,\alpha)(\zeta_1-\alpha)^{i_1}\cdots(\zeta_m-\alpha)^{i_m}$$

are equal to zero whenever

$$\frac{i_1}{r_1}+\cdots+\frac{i_m}{r_m}<\mu-\eta.$$

For the non-zero terms we have

$$\begin{aligned}\left|(\zeta_1-\alpha)^{i_1}\cdots(\zeta_m-\alpha)^{i_m}\right| &< (q_1^{i_1}\cdots q_m^{i_m})^{-\kappa}\\ &= \left[q_1^{i_1/r_1}(q_2^{r_2/r_1})^{i_2/r_2}\cdots(q_m^{r_m/r_1})^{i_m/r_m}\right]^{-r_1\kappa}\\ &\leq \left(q_1^{i_1/r_1}\cdots q_m^{i_m/r_m}\right)^{-r_1\kappa}\\ &< q_1^{-r_1\kappa(\mu-\eta)},\end{aligned}$$

where the first inequality follows from our assumption of $\zeta_1,\ldots,\zeta_m$ as solutions to (9.1), and the third inequality follows from (8.5). By (iii) in Theorem 8.1

$$\begin{aligned}|\phi| &< (r_1+1)\cdots(r_m+1)B_1^{1+3\delta}(1+b_1)^{mr_1}q_1^{-r_1\kappa(\mu-\eta)}\\ &< B_1^{1+5\delta}q_1^{-r_1\kappa(\mu-\eta)},\end{aligned}$$

and by using it once again together with Theorem 4.2 we get

$$\begin{aligned}\left|k_1^{r_1}\cdots k_m^{r_m}\mathrm{No}_{K/\mathbb{Q}}(\phi)\right| &< k_1^{r_1}\cdots k_m^{r_m}\,|\phi|\left|\phi'\right|\cdots\left|\phi^{(N)}\right| < B_1^{1+5\delta}q_1^{-r_1\kappa(\mu-\eta)}B_1^{(N-1)(1+5\delta)}\\ &\times\prod_{i=1}^{m}\left\{k_i\prod_{j=1}^{N}(1+\left|\zeta_i^{(j)}\right|)\right\}^{r_i}\\ &< B_1^{N(1+5\delta)}q_1^{-r_1\kappa(\mu-\eta)}\prod_{i=1}^{m}(6^Nq_i)^{r_i}.\end{aligned}$$

In proof of Theorem 8.1 it was shown that

$$2^{r_1+\cdots+r_m}<B_1^{\delta},$$

so $6^{N(r_1+\cdots+r_m)}<q_1^{\delta Nr_1}$ and by combining all terms we get

$$\begin{aligned}\left|k_1^{r_1}\cdots k_m^{r_m}\mathrm{No}_{K/\mathbb{Q}}(\phi)\right| &< q_1^{\delta N r_1(1+5\delta)+\delta N r_1+mr_1-r_1\kappa(\mu-\eta)}\\ &< q_1^{\delta N r_1(2+5\delta)+mr_1(1+\delta)-r_1\kappa(\mu-\eta)}.\end{aligned}$$

This together with (9.9) implies that

$$\delta N(2+5\delta)+m(1+\delta)>\kappa(\mu-\eta),$$

or

$$\kappa<\frac{\delta N(2+5\delta)+m(1+\delta)}{\mu-\eta},$$

which contradicts (9.4). This proof is thus completed.

□

References

[Hur91] Adolf Hurwitz. Über die angenäherte darstellung der irrationalzahlen durch rationale brüche. *Mathematische Annalen*, 39(2):279–284, 1891.

[Ish08] Daniel Ishak. The thue–siegel–roth theorem, 2008.

[LeV56] William J LeVeque. *Topics in Number Theory, volumes I and II*. Addison-Wesley Publishing Company, Inc, 1956.

[Lio44] Joseph Liouville. "mémoires et communications, 1844.

[Rot55] Klaus Friedrich Roth. Rational approximations to algebraic numbers. *Mathematika*, 2(1):1–20, 1955.