



PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

MASTER THESIS

A version of Siegel's Theorem for quasi-integral points

Author:

Fernanda Cares Cuevas

Supervisor:

[Natalia García Fritz](#)

A thesis submitted in fulfillment of the requirements for the degree of Master in Mathematics in the Faculty of Mathematics of the Pontificia Universidad Católica de Chile.

Jury:

[Daniel Barrera Salazar](#) (Universidad de Santiago de Chile)

[Ricardo Menares Valencia](#) (Pontificia Universidad Católica de Chile)

December 2021

Santiago, Chile

Acknowledgements

Quiero partir dándole las gracias a mi papá que ha sido un pilar fundamental en mi vida y ha estado presente en cada momento. Desde irme a buscar cuando no tenía locomoción hasta apoyarme y aconsejarme en cada decisión que he tomado.

Estoy profundamente agradecida de mi profesora guía, Natalia García, quien me ha acompañado y motivado en este camino desde pregrado. Cada reunión llegaba con dudas y el sentimiento de no haber hecho suficiente, pero sus palabras y guía me daban un camino para seguir adelante y el poder de reconocer mi esfuerzo.

Quiero agradecer a los profesores que conformaron el comité: Daniel Barrera y Ricardo Menares. Sus comentarios mejoraron este documento y también tuve la oportunidad de formarme con ambos.

He tenido muy buenos profesores en esta etapa, me gustaría destacar a Renato Lewin, Giancarlo Urzúa, Héctor Pastén, Alejandro Ramírez y Duván Henao. Gracias a ellos he logrado aprender sobre áreas que me interesan en la matemática, me han ayudado a comprender cosas que pensaba que estaban fuera de mi alcance y me han transmitido su pasión en las áreas que trabajan.

Durante la escritura de esta tesis quiero agradecer a Felipe por los tecitos, comida y apoyo, a Belén por cada llamada telefónica para saber cómo estaba, a Fran y a Fonchi por el espacio seguro y a Bruna por ayudarme con LaTeX y los typos que se me pasaban.

Estoy muy agradecida de mis compañeros durante estos años en la facultad: Sebathon, Vanesa, Dani y Vilches, con quienes disfruté mucho estudiando y no estudiando. También quiero comentar a Cata Encina, Rojo, Jusan, Ceci, Nico Labra y Agus, por el apoyo que he sentido, por cada vez que les pedí un consejo y por el cariño que se ha formado. Por último, a Dani y a Maty que me hacen recordar que ha pasado tiempo desde que entré a la universidad.

Este trabajo fue parcialmente financiado por la beca ANID de Magister Nacional, CONICYT-PFCHA/Magíster Nacional/2020 - 22200632.

Contents

Acknowledgements	i
Introduction	1
1 Preliminaries	3
1.1 Height Functions	3
1.1.1 Absolute Values	3
1.1.2 Heights on number fields	6
1.1.3 Heights on the Projective Space	7
1.1.4 Northcott's Property	8
1.1.5 Height Functions and Geometry	10
1.2 Resultants	11
1.2.1 The Resultant of a Rational Map	11
1.2.2 Application to polynomial systems	12
2 Specific Preliminaries	16
2.1 Quasi-integral points	16
2.1.1 S -integers	16
2.1.2 Definition and Properties	16
2.1.3 Quasi-integrals over \mathbb{Q}	18
2.1.4 Examples and properties.	20
2.1.4.1 $K = \mathbb{Q}$ and $S = \{\infty\}$	20
2.1.4.2 $K = \mathbb{Q}$ and $S = \{\infty, 2\}$	21
2.2 Diophantine Approximation	22
2.3 Arithmetic Dynamics	23
3 Main Theorem	27
3.1 Modified Thue's Theorem	27
3.2 Siegel for quasi-integral points	31

Introduction

From Liouville in 1844 to Roth in 1955 there have been great advances understanding how we can approximate algebraic numbers. These theorems have been extended in various ways: Considering possible nonarchimedean absolute values and working over number fields instead of \mathbb{Q} . We are interested in applications of these theorems, in particular, Thue's and Siegel's Theorem. Siegel proved that there are finitely many integers in the image of a rational function with at least three different poles. This can be generalized to S -integers, where S is a finite set of places over a number field.

Diophantine Approximation's theorems are powerful tools in the area of Arithmetic Dynamics. For example, Silverman in [Sil1] uses Roth's Theorem to prove that there are finitely many S -integers and quasi- (S, ϵ) -integers in orbits of rational functions under some conditions. Gunther and Hindes in [GH] used a generalization of Siegel's Theorem from Levin to prove that there are finitely many elements from \mathcal{O}_S (the integral closure of \mathbb{Z}_S in $\overline{\mathbb{Q}}$) in orbits of rational functions. Even more, they prove that the number of these elements is bounded with a constant that depends only in the function, the function's degree and the set of places S . However, a uniform constant that does not depend on the function can not be achieved for the number of S -integers in orbits of rational maps.

Krieger et al. [KLSTYZ] conjecture that the number of S -units in orbits of rational maps is bounded by a function of $|S|$ and the function's degree. They proved the conjecture for some classes of rational functions and showed that the conjecture follows from the Bombieri-Lang conjecture.

In this work, motivated by trying to generalize some results from [KLSTYZ] to quasi- (S, ϵ) -units we prove a version of Siegel's Theorem for quasi- (S, ϵ) -integers over \mathbb{Q} . Our theorem says that, given a rational function with at least three different poles, there is a constant $c(d)$ depending only on the degree of the function such that for all $0 \leq r < c(d)$ the number of r -quasi-integers in $\phi(\mathbb{Q})$ is finite.

On Chapter 1 we start with definitions and important properties of Height Functions and Resultants that will be key to the proof of the main theorem. On Chapter 2 first we define quasi-integers and provide examples to understand this concept. The compilation of properties and examples that show us that the set of quasi-integral points can not be a ring is original work from the author. Second, we mention the theorems of Diophantine Approximation that we will generalize in this work. In the third place, we present some concepts and results from Arithmetic Dynamics that relate to our main theorem. Finally, on Chapter 3 we prove a modified version of Thue's Theorem and then we use it for the proof of Siegel's Theorem for quasi-integers.

Chapter 1

Preliminaries

1.1 Height Functions

In the definition of S -integers and quasi-integers we will need some way to measure arithmetic complexity. This job is done by the height functions. This concept also appears in the proof of Roth's Theorem and Siegel's Theorem in their general forms. Being both of them important and the motivation for our principal theorem, we will study Height Functions.

1.1.1 Absolute Values

In our search of finding ways to measure numbers we will review the theory of absolute values in number fields. This is not the size function we will be searching for, but it is connected to it in its definition. This section is based on [HinSil, B1]

Definition 1.1.1. [HinSil, B.1] An **absolute value** on a field k is a real-valued function $|\cdot|: k \rightarrow \mathbb{R}$ with the properties:

1. $|x| = 0$ if and only if $x = 0$.
2. $|xy| = |x| \cdot |y| \forall x, y \in k$.
3. $|x + y| \leq |x| + |y| \forall x, y \in k$.

The absolute value is said to be **nonarchimedean** if it satisfies

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

Some classical examples are:

Example 1.1.2. In \mathbb{Q} , $|x|_\infty = \max\{x, -x\}$ is an absolute value.

Example 1.1.3. In \mathbb{Q} , let p be a prime and let x be a rational number. We define $\text{ord}_p(x)$ as the only integer such that $x = p^{\text{ord}_p(x)} \frac{a}{b}$ with $a, b \in \mathbb{Z}$ coprimes and $p \nmid ab$. Then,

$$|x|_p = p^{-\text{ord}_p(x)}$$

is nonarchimedean absolute value.

Definition 1.1.4. Two absolute values $|\cdot|_1, |\cdot|_2$ on a field k are **equivalent** if there exists some $\lambda > 0$ such that $|\cdot|_1 = |\cdot|_2^\lambda$.

Definition 1.1.5. We define a **place** of K as an equivalent class of the set of absolute values where two absolute values are related if and only if they are equivalent.

By Ostrowski's theorem, any non trivial absolute value on \mathbb{Q} is equivalent to some of the examples above.

To simplify things we are going to work on number fields. From now on K will denote a finite algebraic extension of \mathbb{Q} .

We will denote:

- $M_{\mathbb{Q}} = \{\infty, 2, 3, 5, \dots\}$
- M_K as the set of all absolute values whose restriction to \mathbb{Q} is in $M_{\mathbb{Q}}$.

Lemma 1.1.6 (Product formula). *For all $x \in \mathbb{Q}^\times$,*

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1.$$

Proof. By the multiplicative property from absolute values, it is enough to prove the formula for some prime p . If we evaluate p in the absolute values we have:

- $|p|_p = p^{-1} = \frac{1}{p}$,
- $|p|_\infty = p$,
- if q is a prime different than p : $|p|_q = 1$.

So, the multiplication is 1. ■

We can define an absolute value in some finite extension of K using the norm and some absolute value on K :

Proposition 1.1.7. *Let L/K be a finite extension of fields. Then an absolute value $|\cdot|_v$ on K can be extended to L in the following way*

$$|x| := |\text{Norm}_{L/K}(x)|^{\frac{1}{[L:K]}}.$$

Notice that it is an extension because $|\text{Norm}_{L/K}(x)| = x^{[L:K]}$ if $x \in K$.

Using this definition we can extend an absolute value $|\cdot|_v$ on K to $\overline{\mathbb{Q}}$. This is well defined, in the sense that for each $\alpha \in \overline{\mathbb{Q}}$ it does not depend on the choice of the finite extension L with $\alpha \in L$. The latter lies in the fact that given $L_1/L_2/K$ finite extensions then $\text{Norm}_{L_2/K} \circ \text{Norm}_{L_1/L_2} = \text{Norm}_{L_1/K}$.

Remark 1.1.8. In general, over a place $|\cdot|_v$ on K there are many $|\cdot|_w$ on L extending $|\cdot|_v$. In this case, we will denote $w | v$ or we will say w is over v .

The next property will be useful to prove some definitions are well-defined.

Proposition 1.1.9. [*Neu, II. Corollary 8.4*] *If L/K is separable, then one has*

$$[L : K] = \sum_{w|v} [L_w : K_v],$$

where K_v is the completion of K with respect to $|\cdot|_v$. For norms we have:

$$\text{Norm}_{L/K}(x) = \prod_{w|v} \text{Norm}_{L_w/K_v}(x).$$

We will use the previous property immediately:

Lemma 1.1.10 (Product formula). [*HinSil, Proposition B.1.2*] *Let K be a number field. There exist a set of places of K that we will denote M_K such that for all $x \in K^\times$*

$$\prod_{v \in M_K} |x|_v^{d_v} = 1,$$

where $d_v = [K_v : \mathbb{Q}_v]$.

Proof. For every $v \in M_{\mathbb{Q}}$, we extend the absolute value to K like in Proposition 1.1.7. Since every absolute value from M_K is an extension to some absolute value from $M_{\mathbb{Q}}$, we have

$$\prod_{w \in M_K} |x|_w^{d_w} = \prod_{v \in M_{\mathbb{Q}}} \prod_{\substack{w \in M_K \\ w|v}} |\text{Norm}_{K/\mathbb{Q}}(x)|_v^{\frac{d_w}{[L:K]}}.$$

By Proposition 1.1.9 the latter is equal to $\prod_{p \in M_{\mathbb{Q}}} |\text{Norm}_{K/\mathbb{Q}}(x)|_v$ and the product formula in \mathbb{Q} (1.1.6) says that it is 1. ■

1.1.2 Heights on number fields

Here we define heights over number fields and present some basic properties.

Definition 1.1.11. Let $\alpha \in \overline{\mathbb{Q}}$ and K a number field such that $\alpha \in K$. The **(multiplicative) height** of α is

$$H(\alpha) := \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{d_v/d},$$

where $d_v = [K_v : \mathbb{Q}_v]$ and $d = [K : \mathbb{Q}]$.

We also define the **logarithmic height** of α :

$$h(\alpha) = \log(H(\alpha)) = \sum_{v \in M_K} \frac{d_v}{d} \log \max\{1, |\alpha|_v\}.$$

Lemma 1.1.12. *The logarithmic height $h(\alpha)$ is well-defined (and so it is the multiplicative height).*

Proof. Suppose $\alpha \in K$. Let L/K be a finite extension. We will prove that $h(\alpha)$ does not depend on the choice of field.

If we first use the definition of the height of α with the number field L then

$$\begin{aligned} h(\alpha) &= \sum_{w \in M_L} \frac{[L_w : \mathbb{Q}_w]}{[L : \mathbb{Q}]} \log \max\{1, |\alpha|_w\} \\ &= \frac{1}{[L : K][K : \mathbb{Q}]} \sum_{w \in M_L} [L_w : K_w][K_w : \mathbb{Q}_w] \log \max\{1, |\alpha|_w\} \quad \text{where } v = w|_K \\ &= \frac{1}{[L : K][K : \mathbb{Q}]} \sum_{v \in M_K} \sum_{w|v} [L_w : K_w][K_w : \mathbb{Q}_w] \log \max\{1, |\alpha|_v\} \\ &= \frac{1}{[L : K][K : \mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max\{1, |\alpha|_v\} \underbrace{\sum_{w|v} [L_w : K_w]}_{=[L:K]} \quad \text{by 1.1.9} \\ &= \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log \max\{1, |\alpha|_v\}, \end{aligned}$$

where the last expression is the definition of $h(\alpha)$ if we use the number field K . ■

Lemma 1.1.13. *For $\alpha \in \mathbb{Q}$, we write $\alpha = \frac{a}{b}$ where a, b are coprime integers. Then*

$$H(\alpha) = \max\{|a|_{\infty}, |b|_{\infty}\}.$$

Proof. Using $K = \mathbb{Q}$ in the Definition 1.1.11 we have $d_v = d = 1$ for all $v \in \mathbb{Q}$. So,

$$\begin{aligned} H(\alpha) &= \prod_{v \in M_{\mathbb{Q}}} \max\{1, |\alpha|_v\} \\ &= \underbrace{\prod_{v \in M_{\mathbb{Q}}} |b|_v}_{=1} \cdot \prod_{v \in M_{\mathbb{Q}}} \max\{1, |\alpha|_v\} \quad (\text{by Lemma 1.1.6}) \\ &= \prod_{v \in M_{\mathbb{Q}}} \max\{|a|_v, |b|_v\}. \end{aligned}$$

As a, b are coprime integers, for every prime p we have $\max\{|a|_p, |b|_p\} = 1$. So the previous product is equal to $\max\{|a|_{\infty}, |b|_{\infty}\}$. ■

Proposition 1.1.14.

1. $H(\alpha) \geq 1$ and $h(\alpha) \geq 0$ for all $\alpha \in \overline{\mathbb{Q}}$.
2. If $u^n = 1$, then $H(u) = 1$. In particular, $H(1) = 1$.

Proof. The first is because in the definition we are multiplying numbers that are greater than or equal to 1. Indeed, $\max\{1, |\alpha|_v\} \geq 1$ for all $v \in M_K$. The second follows from the fact that for every absolute value v if $u^n = 1$ then $|u|_v = 1$. ■

Lemma 1.1.15 (Finiteness Property in \mathbb{Q}). *Given $B \geq 0$, there are finitely many rational numbers such that their height is bounded above by B .*

1.1.3 Heights on the Projective Space

From the notion of height on number fields one can define heights on the projective space as follows:

Definition 1.1.16. [HinSil, B.2] Let K be a number field, and let

$$P = [x_0, x_1, \dots, x_n] \in \mathbb{P}^n(K)$$

be a point whose homogeneous coordinates are chosen in K . The **height** of P is the quantity

$$H(P) = \prod_{v \in M_K} \max\{|x_0|_v, |x_1|_v, \dots, |x_n|_v\}^{d_v/d},$$

where $d_v = [K_v : \mathbb{Q}_v]$ and $d = [K : \mathbb{Q}]$

Remark 1.1.17. [HinSil, B.2] It is analogous to the case of heights over a number field to prove that the definition does not depend on the field chosen. However, we have to

prove that it is also independent of the choice of homogeneous coordinates for P . By the product formula (1.1.10), if $c \in K, c \neq 0$ we have

$$\begin{aligned} \prod_{v \in M_K} \max\{|cx_0|_v, |cx_1|_v, \dots, |cx_n|_v\}^{d_v} &= \prod_{v \in M_K} \underbrace{|c|_v^{d_v}}_{=1} \prod_{v \in M_K} \max\{|x_0|_v, |x_1|_v, \dots, |x_n|_v\}^{d_v} \\ &= \prod_{v \in M_K} \max\{|x_0|_v, |x_1|_v, \dots, |x_n|_v\}^{d_v}. \end{aligned}$$

Lemma 1.1.18. [Sil2, Remark 3.5] For $P = [x_0, x_1, \dots, x_n] \in \mathbb{P}^n(\mathbb{Q})$ with homogeneous coordinates satisfying $x_i \in \mathbb{Z}$ and $\gcd(x_i) = 1$ we have

$$H(P) = \max\{|x_0|_\infty, \dots, |x_n|_\infty\}.$$

Proof. Let p be a prime. As $x_i \in \mathbb{Z}$, one has $|x_i|_p \leq 1$ for each i and $|x_i|_p = 1$ for at least one i . Then in the product

$$\prod_{v \in M_{\mathbb{Q}}} \max\{|x_0|_v, |x_1|_v, \dots, |x_n|_v\}$$

the only term that contributes is the one corresponding to the archimedean absolute value. ■

Lemma 1.1.19 (Finiteness Property in $\mathbb{P}^n(\mathbb{Q})$). Given $B \geq 0$, the set

$$\{P \in \mathbb{P}^n(\mathbb{Q}) : H(P) \leq B\}$$

is finite.

1.1.4 Northcott's Property

A useful property of heights is the finiteness property we proved over \mathbb{Q} and $\mathbb{P}^n(\mathbb{Q})$ in the previous sections. Now we will prove it in general but we need to add conditions to the degree of the point. This property is called Northcott Property.

For this we will need the following theorem:

Theorem 1.1.20. [Sil2, Theorem 3.6] Let K/\mathbb{Q} be a number field, let $\alpha \in \overline{K}$ and consider $\sigma \in \text{Gal}(\overline{K}/K)$. Then $H(\sigma(\alpha)) = H(\alpha)$. In other words, the height is invariant under the action of the Galois group.

Theorem 1.1.21 (Northcott's Property). *Let K/\mathbb{Q} be a number field, and let B, D be any real constants. Then the set*

$$\{\alpha \in \overline{\mathbb{Q}} : H(\alpha) \leq B \text{ and } [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq D\}$$

is finite. In other words, there are only finitely many numbers in $\overline{\mathbb{Q}}$ of bounded height and bounded degree.

Proof. This proof is adapted from [Sil2, Theorem 3.7].

Suppose $\alpha \in \overline{\mathbb{Q}}$ with $H(\alpha) \leq B$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ where $d \leq D$. Let

$$F(x) = x^d + a_1x^{d-1} + \cdots + a_d \in \mathbb{Q}[x]$$

be the minimal polynomial of α . Let

$$F(x) = (x - \alpha_1) \cdots (x - \alpha_d)$$

be the factorization of F over $\mathbb{C}[x]$. As $\alpha_1, \dots, \alpha_d$ are the conjugates of α , Theorem 1.1.20 tell us that

$$H(\alpha_1) = \cdots = H(\alpha_d) = H(\alpha).$$

Recall that the coefficients of F are the elementary symmetric polynomials of the roots (up to sign). For example, $a_1 = -(\alpha_1 + \cdots + \alpha_d)$ and $a_d = (-1)^d \alpha_1 \cdots \alpha_d$.

More generally, we have

$$a_k = (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq d} \alpha_{i_1} \cdots \alpha_{i_k}.$$

Using the triangle inequality, for any $v \in M_{\mathbb{Q}(\alpha)}$ we have

$$\begin{aligned} |a_k|_v &= \left| \sum_{1 \leq i_1 < \cdots < i_k \leq d} \alpha_{i_1} \cdots \alpha_{i_k} \right|_v \\ &\leq \binom{d}{k} \max_{1 \leq i_1 < \cdots < i_k \leq d} |\alpha_{i_1} \cdots \alpha_{i_k}|_v \\ &\leq \binom{d}{k} \max\{|\alpha_1|_v, 1\} \cdots \max\{|\alpha_d|_v, 1\}. \end{aligned}$$

Taking the maximum over k and using the fact that $\binom{d}{k} \leq 2^d$ for all k , we find that

$$\max\{1, |a_1|_v, \dots, |a_d|_v\} \leq 2^d \max\{|\alpha_1|_v, 1\} \cdots \max\{|\alpha_d|_v, 1\}.$$

If we raise to the d_v -th power, multiply over all v , and take the d -th root, we obtain

$$H([1, a_1, \dots, a_d]) \leq 2^d H(\alpha_1) \cdots H(\alpha_d).$$

By Theorem 1.1.20 and the fact that $H(\alpha) \leq B$ we conclude that

$$H([1, a_1, \dots, a_d]) \leq (2B)^d \leq (2B)^D.$$

Recall that every $a_i \in \mathbb{Q}$, so by Lemma 1.1.19 there are only finitely many possibilities for a_1, \dots, a_n . Hence there are only finitely many possibilities for the minimal polynomial of α , and since each F has only d roots, there are only finitely many possibilities for α . This proves that the set is finite. ■

Our first application of this theorem is the following

Theorem 1.1.22 (Kronecker Theorem). [Sil2, Theorem 3.8] *Let $\alpha \in \overline{\mathbb{Q}}$ be a nonzero algebraic number. Then*

$$H(\alpha) = 1 \quad \text{if and only if } \alpha \text{ is a root of unity.}$$

Proof. We have seen in Proposition 1.1.14 that if $\alpha^n = 1$ for some $n \geq 1$, then $H(\alpha) = 1$. Now suppose that $H(\alpha) = 1$, from the definition of the height we have

$$H(x^n) = H(x)^n$$

for all $x \in \overline{\mathbb{Q}}$ and all $n \geq 1$. So, $H(\alpha^n) = H(\alpha)^n = 1$ and the set

$$\{\alpha^n : n \in \mathbb{Z}, n \geq 1\}$$

has bounded height (by 1). From Theorem 1.1.21 and the fact that this set is in the number field $\mathbb{Q}(\alpha)$ (so, it has bounded degree), we have that the set of positive powers of α is finite. Finally, there are integers $i > k > 0$ such that $\alpha^i = \alpha^k$ and, as $\alpha \neq 0$, then α is a root of unity. ■

1.1.5 Height Functions and Geometry

This section will be based on [Sil2, 3.2].

Definition 1.1.23. A **rational map** of degree d between projective spaces is a map

$$\begin{aligned} \phi : \mathbb{P}^N &\rightarrow \mathbb{P}^M \\ \phi(P) &= [f_0(P), \dots, f_M(P)], \end{aligned}$$

where $f_0, \dots, f_M \in \overline{K}[x_0, \dots, x_N]$ are homogeneous polynomials of degree d with no common factors. The rational map ϕ is **defined in P** if at least one of the values $f_0(P), \dots, f_M(P)$ is nonzero. The rational map ϕ is called a **morphism** if it is defined at every point of $\mathbb{P}^N(\overline{K})$. If the polynomials f_0, \dots, f_M have coefficients in K , we say that ϕ is **defined over K** .

In this section our goal is to compare the value of $H(P)$ and $H(\phi(P))$ for a rational map ϕ . This result uses an important theorem from algebraic geometry called the Nullstellensatz.

Theorem 1.1.24. [Sil2, Theorem 3.11] *Let $\phi : \mathbb{P}^N(\overline{K}) \rightarrow \mathbb{P}^M(\overline{K})$ be a morphism of degree d . Then there are constants $C_1, C_2 > 0$, depending on ϕ , such that*

$$C_1 H(P)^d \leq H(\phi(P)) \leq C_2 H(P)^d \quad \text{for all } P \in \mathbb{P}^N(\overline{K}).$$

In fact, the upper bound is valid for rational maps provided we restrict our attention to points P at which ϕ is defined.

1.2 Resultants

1.2.1 The Resultant of a Rational Map

This section is based on [Sil2, 2.4].

In this section we will consider rational maps $\phi : \mathbb{P}^1 \rightarrow \mathbb{P}^1$. By definition ϕ is given by a pair of homogeneous polynomials

$$\phi = [F(x, y), G(x, y)]$$

having no nontrivial common roots. However, if we reduce F and G modulo some prime, they may acquire common roots in the residue field. The resultant is a useful tool to understand this phenomenon.

Proposition 1.2.1. [Sil2, Proposition 2.13] *Let*

$$\begin{aligned} P(x, y) &= a_0 x^n + a_1 x^{n-1} y + \dots + a_{n-1} x y^{n-1} + a_n y^n \\ Q(x, y) &= b_0 x^m + b_1 x^{m-1} y + \dots + b_{m-1} x y^{m-1} + b_m y^m \end{aligned}$$

be homogeneous polynomials of degrees n and m with coefficients in a field K . There exists a polynomial

$$\text{Res}(a_0, \dots, a_n, b_0, \dots, b_m) \in \mathbb{Z}[a_0, \dots, a_n, b_0, \dots, b_m],$$

Lemma 1.2.2. [CLO][Lemma 6,3.§5] Let k be a field. Let $F, G \in k[x]$ polynomials of degrees $n > 0$ and $m > 0$, respectively. Then F and G have a common factor if and only if there are polynomials $A, B \in k[x]$ such that

1. A and B are not both zero.
2. A has degree at most $m - 1$ and B has degree at most $n - 1$
3. $AF + BG = 0$.

Suppose $A = c_0x^{m-1} + \cdots + c_{m-1}$ and $B = d_0x^{n-1} + \cdots + d_{n-1}$. Asking whether F, G have a common factor is equivalent to finding $c_i, d_i \in k$, not all zero such that $AF + BG = 0$. To get a system of linear equations we can write

$$F = a_0x^n + \cdots + a_n, \quad a_0 \neq 0$$

$$G = b_0x^m + \cdots + b_m, \quad b_0 \neq 0,$$

where $a_i, b_i \in k$. With this information, finding c_i, d_i is equivalent to solve the system of linear equations given by $AF + BG = 0$. Which has $n + m$ equations and $n + m$ unknowns. From linear algebra, there is a non zero solution if and only if the coefficient matrix has determinant zero.

Definition 1.2.3. [CLO][Definition 7,3.§5] Given polynomials $F, G \in k[x]$ of positive degree, write them in the form

$$F = a_0x^n + \cdots + a_n, \quad a_0 \neq 0$$

$$G = b_0x^m + \cdots + b_m, \quad b_0 \neq 0,$$

We can adapt the theory of resultants to the case of polynomials in two variables. Suppose we are given $F, G \in k[x, y]$ of positive degree in x . We write

$$F = a_0x^n + \cdots + a_n, \quad a_0 \neq 0$$

$$G = b_0x^m + \cdots + b_m, \quad b_0 \neq 0,$$

where $a_i, b_i \in k[y]$, and we define the resultant of F and G with respect to x to be the determinant of the Sylvester matrix of F and G with respect of x .

Example 1.2.6. Let $F(x, y) = x^3 + 2xy + y^3$ and $G(x, y) = x^2 + xy^2$, then

$$\text{Res}_x(F, G) = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & y^2 & 1 & 0 \\ 2y & 0 & 0 & y^2 & 1 \\ y^3 & 2y & 0 & 0 & y^2 \\ 0 & y^3 & 0 & 0 & 0 \end{vmatrix} = -y^9 - y^6.$$

Proposition 1.2.7. [CLO, Proposition 1, 3.§6] Let $F, G \in k[x, y]$ have positive degree as polynomials in x . Then $\text{Res}_x(F, G) = 0$ if and only if F and G have a common factor in $k[x, y]$ which has positive degree in x .

Corollary 1.2.8. If $F, G \in \mathbb{C}[x]$, then $\text{Res}_x(F, G) = 0$ if and only if F and G have a common root in \mathbb{C} .

Example 1.2.9. Let $F(x, y) = x^3 + 2xy + y^3$ and $G(x, y) = x^2 + xy^2$, then in the previous example we calculated

$$\text{Res}_x(F, G) = -y^9 - y^6 = -y^6(y^3 + 1).$$

The proposition tells us if $a, b \in \mathbb{C}$ are such that $F(a, b) = G(a, b) = 0$, then b is such that $\text{Res}_x(F, G)(b) = 0$. So, $b \in \{0, -1, \frac{1+i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}\}$. To find a we solve

$$F(x, b) = G(x, b) = 0$$

for each possible b .

Chapter 2

Specific Preliminaries

2.1 Quasi-integral points

2.1.1 S -integers

Here we introduce the notion of sets of S -integers, which are rings of arithmetic interest. We will understand why the word integer is in the name with the example we provide. Later, we will generalize with concept with the set of quasi-integers.

Definition 2.1.1. [HinSil, B.1] Let $S \subseteq M_K$ be any set of absolute values containing the archimedean absolute values, then the ring of S -integers of K is defined to be

$$R_S := \{x \in K : |x|_v \leq 1 \text{ for all } v \in M_K, v \notin S\}.$$

Remark 2.1.2. The set defined above is a ring. By the multiplicative property of absolute values, it is closed under product. As every $v \notin S$ is nonarchimedean, the strong triangle inequality implies it is closed under addition.

Example 2.1.3. If $S = \{\infty\}$, then the S -integers are \mathbb{Z} . Indeed, no prime number can divide the denominator of a S -integer because its p -adic absolute value is less than or equal to 1 for every prime p .

2.1.2 Definition and Properties

Definition 2.1.4. [HsiaSil] Let K/\mathbb{Q} be a number field, let S be a finite set of places of K and let $1 \geq \epsilon > 0$. An element $x \in K$ is said to be **quasi- (S, ϵ) -integral** if

$$\sum_{v \in S} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |x|_v\} \geq \epsilon h(x). \quad (2.1)$$

Lemma 2.1.5. *An element $x \in K$ is in the set of S -integers of K if and only if x is a quasi- $(S,1)$ -integral, in which case (2.1) is an equality.*

Proof. In the first place, if $x \in R_S$, then $|x|_v \leq 1$ for all $v \notin S$. So, $\log \max\{1, |x|_v\} = 0$ for all $v \notin S$. By definition of height,

$$\begin{aligned} h(x) &= \sum_{v \in M_K} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |x|_v\} \\ &= \sum_{v \in S} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |x|_v\}, \end{aligned}$$

where we are using the fact that $x \in R_S$ in the last equality. In particular,

$$\sum_{v \in S} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |x|_v\} \geq h(x).$$

Conversely, if x is a quasi- $(S, 1)$ -integer, then

$$\sum_{v \notin S} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |x|_v\} \leq 0.$$

As $\log \max\{1, |x|_v\} \geq 0$ for every $v \in M_K$, the previous inequality is true only if $|x|_v \leq 1$ for all $v \notin S$. By definition, $x \in R_S$. ■

Remark 2.1.6. Fix K/\mathbb{Q} a number field and a finite set $S \subseteq M_K$, we will denote by $R_{S,\epsilon}$ the set of elements in K that are quasi- (S, ϵ) -integers.

Lemma 2.1.7. *Given $0 < \epsilon < \epsilon' \leq 1$, we have that $R_{S,\epsilon'} \subseteq R_{S,\epsilon}$.*

So, it is interesting to study the properties of the numbers that are quasi- (S, ϵ) -integers for some $0 < \epsilon \leq 1$.

Proposition 2.1.8. *Given K/\mathbb{Q} a number field and a finite set $S \subseteq M_K$, we have*

$$\bigcup_{0 < \epsilon \leq 1} R_{S,\epsilon} = K \setminus \{x \in K : |x|_v \leq 1 \forall v \in S, x \neq 0 \text{ and } x^n \neq 1 \forall n \geq 1\}.$$

Proof. Suppose that $x \notin R_{S,\epsilon}$ for all $0 < \epsilon \leq 1$, then

$$\sum_{v \in S} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |x|_v\} < \epsilon h(x), \quad \forall 0 < \epsilon \leq 1. \quad (2.2)$$

Making $\epsilon \rightarrow 0$, we have

$$\sum_{v \in S} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |x|_v\} \leq 0,$$

which implies that $|x|_v \leq 1$ for all $v \in S$. Even more, (2.2) tells us that $h(x) \neq 0$. By 1.1.22, $x \neq 0$ and x is not a root of unity.

Conversely, suppose $x \in K, x \neq 0, x$ is not a root of unity and $|x|_v \leq 1$ for all $v \in S$. Again by Theorem 1.1.22 we know that $h(x) \neq 0$. Notice that $|x|_v \leq 1$ for all $v \in S$ and $h(x) > 0$ makes that

$$0 = \sum_{v \in S} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |x|_v\} < \epsilon h(x), \quad \forall 0 < \epsilon \leq 1.$$

Finally, x is not a quasi- (S, ϵ) -integer for all $0 < \epsilon \leq 1$. ■

Definition 2.1.9. Let K/\mathbb{Q} be a number field, let S be a finite set of places of K and let $0 < \epsilon \leq 1$. A nonzero element $x \in K$ is said to be a **quasi- (S, ϵ) -unit** if x, x^{-1} are quasi- (S, ϵ) -integers. We will denote by $R_{S, \epsilon}^*$ the set of elements in K that are quasi- (S, ϵ) -units.

2.1.3 Quasi-integrals over \mathbb{Q}

Working over \mathbb{Q} we have a compact and immediate way to see if a number is a quasi- (S, ϵ) -integer or not.

Proposition 2.1.10. Let $S = \{\infty, p_1, \dots, p_r\} \subseteq M_{\mathbb{Q}}$ be a finite set of absolute values from \mathbb{Q} . Let $\alpha = \frac{a}{b}$ where a, b have no common factors. Write $b = p_1^{\alpha_1} \cdots p_r^{\alpha_r} k$, where $\alpha_i \geq 0$ and $p_i \nmid k$ for all i . Then, given $0 < \epsilon \leq 1$,

$$\alpha \in R_{S, \epsilon} \quad \text{if and only if} \quad H(\alpha)^{1-\epsilon} \geq |k|.$$

Recall that the height function on \mathbb{Q} is easy to calculate from Lemma 1.1.13.

Proof. By definition $\alpha \in R_{S, \epsilon}$ if and only if

$$\begin{aligned} \sum_{v \in S} \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log \max\{1, |x|_v\} &\geq \epsilon h(x) \\ \Leftrightarrow \prod_{v \in S} \max\{1, |x|_v\} &\geq H(\alpha)^\epsilon \\ \Leftrightarrow \max\{1, |x|_\infty\} \prod_{i=1}^r \max\{1, |x|_{p_i}\} &\geq H(\alpha)^\epsilon. \end{aligned}$$

Define $b' := p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, then

$$\prod_{i=1}^r \max\{1, |x|_{p_i}\} = b'.$$

We have $\alpha \in R_{S,\epsilon}$ if and only if

$$\max\{1, |\alpha|_\infty\} |b'| \geq H(\alpha)^\epsilon.$$

Lets branch into cases, we will denote $|\cdot| := |\cdot|_\infty$:

- If $|\alpha|_\infty \geq 1$, then $H(\alpha) = |\alpha|$. We have the inequality

$$\max\{1, |\alpha|\} |b'| = \frac{|\alpha|}{|k|} \geq H(\alpha)^\epsilon = |\alpha|^\epsilon$$

if and only if

$$|k| \leq |\alpha|^{1-\epsilon} = H(\alpha)^{1-\epsilon}.$$

- If $|\alpha|_\infty \leq 1$, then $H(\alpha) = |b|$. We have the inequality

$$\max\{1, |\alpha|\} |b'| = |b'| \geq H(\alpha)^\epsilon = |b|^\epsilon$$

if and only if

$$|k| \leq |b|^{1-\epsilon} = H(\alpha)^{1-\epsilon},$$

where in the last line we multiplied by $|k|$ and used that $b = b'k$.

We conclude that α is a quasi- (S, ϵ) -integer if and only if $|k| \leq H(\alpha)^{1-\epsilon}$. ■

In the literature there is another definition of quasi-integral points over \mathbb{Q} :

Definition 2.1.11. For $\alpha \in \mathbb{Q}$ we write $\alpha = \frac{a}{b}$ where a, b are coprime integers. Let $r \geq 0$, then α is r -quasi-integral if

$$|b| \leq H(\alpha)^r.$$

Remark 2.1.12. With the Proposition 2.1.10 we note that the last definition is not something new. Indeed, α is r -quasi-integral if and only if α is a quasi- $(\{\infty\}, 1 - r)$ -integer.

We will differentiate them by the place where we put the r or ϵ .

We prefer to use the Definition 2.1.11 on the results we will prove in this thesis because it has the property that if r grows, then the set of r -quasi-integral points grows (contrary to quasi- (S, ϵ) -integers).

2.1.4 Examples and properties.

Our goal in this section is to fix ideas about the concept of quasi- (S, ϵ) -integers and have some counterexamples for properties that R_S have and $R_{S, \epsilon}$ can not have. The most important of them is that $R_{S, \epsilon}$ may not be a ring, even if we consider $\bigcup_{0 < \epsilon \leq 1} R_{S, \epsilon}$.

From now on we will work over \mathbb{Q} , so it is convenient to write the Proposition 2.1.10 in another way:

Proposition 2.1.13. *Let $S = \{\infty, p_1, \dots, p_r\} \subseteq M_{\mathbb{Q}}$ be a finite set of absolute values from \mathbb{Q} including the archimedean one. Let $\alpha = \frac{a}{b}$ where a, b have no common factors. Write $b = p_1^{\alpha_1} \cdots p_r^{\alpha_r} k$, where $\alpha_i \geq 0$ and $p_i \nmid k$ for all i . Then, given $0 < \epsilon \leq 1$ and $H(\alpha) \neq 0$,*

$$\alpha \in R_{S, \epsilon} \quad \text{if and only if} \quad \epsilon \leq 1 - \frac{\log |k|}{\log H(\alpha)}.$$

Proof. Apply log over Proposition 2.1.10 and isolate ϵ . ■

2.1.4.1 $K = \mathbb{Q}$ and $S = \{\infty\}$

As there are not primes in S , the Proposition 2.1.13 translates into

$$\alpha \in R_{\infty, \epsilon} \quad \text{if and only if} \quad \epsilon \leq 1 - \frac{\log |b|}{\log H(\alpha)},$$

where $\alpha = \frac{a}{b}$ in lowest terms.

Note that if $|b| \geq H(\alpha)$ (or, equivalently, $H(\alpha) = |b|$) then there is no $\epsilon > 0$ that satisfies

$$\epsilon \leq 1 - \frac{\log |b|}{\log H(\alpha)}.$$

It follows that if $|\alpha| \leq 1$ and $\alpha \notin \{0, 1, -1\}$ then $\alpha \notin R_{S, \epsilon}$ for all $0 < \epsilon \leq 1$. This is not new because we proved in Proposition 2.1.8 that $\{x \in \mathbb{Q} : |x|_{\infty} \leq 1, x \neq 0, 1, -1\}$ is the complement of $\bigcup_{0 < \epsilon \leq 1} R_{S, \epsilon}$.

Example 2.1.14.

1. $-\frac{4}{3} \in R_{S, \epsilon}$ if and only if $\epsilon \leq 1 - \frac{\log 3}{\log 4} \approx 0.2075$.
2. $\frac{5}{4} \in R_{S, \epsilon}$ if and only if $\epsilon \leq 1 - \frac{\log 4}{\log 5} \approx 0.138$.
3. $\frac{31}{12} \in R_{S, \epsilon}$ if and only if $\epsilon \leq 1 - \frac{\log 12}{\log 31} \approx 0.276$.

Remark 2.1.15. Given $0 < \epsilon < 1$, the set $R_{S,\epsilon}$ may not be closed under addition. For example, $-\frac{4}{3}, \frac{31}{12} \in R_{\{\infty\},0.2}$ but

$$\frac{5}{4} = \frac{31}{12} + -\frac{4}{3} \notin R_{\{\infty\},0.2}.$$

2.1.4.2 $K = \mathbb{Q}$ and $S = \{\infty, 2\}$

With the notation from Proposition 2.1.13, we have in this case that $b' = 2^{\text{ord}_2(b)}$ so the condition translates into

$$\alpha \in R_{\infty,\epsilon} \quad \text{if and only if} \quad \epsilon \leq 1 + \frac{\text{ord}_2(b) \log 2 - \log |b|}{\log H(\alpha)},$$

where $\alpha = \frac{a}{b}$ in lowest terms.

This is because $\log |k| = \log \frac{|b|}{b'} = \log |b| - \log(2) \cdot \text{ord}_2(b)$.

Example 2.1.16.

1. $-\frac{4}{3} \in R_{S,\epsilon}$ if and only if $\epsilon \leq 1 - \frac{\log 3}{\log 4} \approx 0.2075$.
2. $\frac{3}{4} \in R_{S,\epsilon}$ for every $0 < \epsilon \leq 1$.
3. $\frac{5}{6} \in R_{S,\epsilon}$ if and only if $\epsilon \leq \frac{\log 2}{\log 6} \approx 0.3868$.
4. $\frac{6}{5} \in R_{S,\epsilon}$ if and only if $\epsilon \leq 1 - \frac{\log 5}{\log 6} \approx 0.1017$.
5. $\frac{1}{2} \in R_{S,\epsilon}$ for every $0 < \epsilon \leq 1$.

Remark 2.1.17. Given $0 < \epsilon < 1$, the set $R_{S,\epsilon}$ may not be closed under product. For example, $\frac{4}{3}, \frac{1}{2} \in R_{\{\infty,2\},0.2}$ but

$$\frac{2}{3} = \frac{1}{2} \cdot \frac{4}{3} \notin R_{\{\infty,2\},\epsilon},$$

for every $0 < \epsilon \leq 1$.

Even more, $\bigcup_{0 < \epsilon \leq 1} R_{S,\epsilon}$ may not be closed for the product.

Remark 2.1.18. It is possible that $\bigcup_{0 < \epsilon \leq 1} R_{S,\epsilon}$ may not be closed under addition. For example, $\frac{5}{6}, -\frac{1}{2} \in R_{\{\infty,2\},0.382}$, but

$$\frac{1}{3} = \frac{5}{6} + -\frac{1}{2} \notin R_{\{\infty,2\},\epsilon},$$

for every $0 < \epsilon \leq 1$.

Remark 2.1.19. Given $0 < \epsilon < 1$, $R_{S,\epsilon}^*$ may not be closed under product. For example, $\frac{4}{3}, \frac{5}{6} \in R_{\{\infty,2\},0.1}^*$, but

$$\frac{10}{9} = \frac{4}{3} \cdot \frac{5}{6} \in R_{\{\infty,2\},\epsilon}^*,$$

if and only if $0 < \epsilon \leq 1 - \frac{\log 9}{\log 10} \approx 0.045$. In particular, $\frac{10}{9} \notin R_{\{\infty,2\},0.1}^*$.

2.2 Diophantine Approximation

Our results will be based in many of the theorems in this section. Diophantine Approximation is a crucial tool in the theorems from the area of Arithmetic Dynamics that we studied in this thesis and it is an area of interest of its own. This section will be based in [Sil2, 3.6].

Let K be a number field and let S be a finite set of absolute values on K .

Theorem 2.2.1 (Roth). [Sil2, Theorem 3.40] *Let $\varepsilon > 0$. For each $v \in S$, extend v to \overline{K} in some fashion and choose an algebraic number $\alpha_v \in \overline{K}$. Then there is a constant $\kappa > 0$, depending on K, S, ε and $\{\alpha_v\}_{v \in S}$ such that*

$$\prod_{v \in S} \min\{|z - \alpha_v|_v, 1\}^{d_v} \geq \frac{\kappa}{H(z)^{d(2+\varepsilon)}} \quad \text{for all } z \in K.$$

Roth's Theorem has as a consequence Thue's Theorem. We will prove a modified version of the case $K = \mathbb{Q}$ and $S = \{\infty\}$ in Chapter 3.

Theorem 2.2.2 (Thue-Mahler). [Sil2, Theorem 3.41] *Let $G(x, y) \in K[x, y]$ be a homogeneous polynomial with at least three distinct roots in $\mathbb{P}^1(\mathbb{C})$, and let $B \in K$. Then there are only finitely many $(x, y) \in R_S^2$ satisfying $G(x, y) = B$.*

Our main result in this thesis is a generalization of the following theorem:

Theorem 2.2.3 (Siegel). [Sil2, Theorem 3.42] *Let $\phi(z) \in K(z)$ be a rational function with at least three distinct poles in \overline{K} . Then there are only finitely many $\alpha \in K$ satisfying $\phi(\alpha) \in R_S$.*

Proof. We will prove this in the case of $K = \mathbb{Q}$ and $S = \{\infty\}$.

In the first place, we write

$$\phi = [F(x, y), G(x, y)]$$

where $F(x, y), G(x, y) \in \mathbb{Z}[x, y]$ are homogeneous polynomials of degree d with no common factors. So, for any $\alpha = \frac{a}{b} \in \mathbb{Q}$ written in lowest terms, we have

$$\phi(\alpha) = \frac{F(a, b)}{G(a, b)}.$$

Then $\phi(\alpha) \in \mathbb{Z}$ if and only if $G(a, b)$ divides $F(a, b)$.

Recall from Proposition 1.2.1 that, as F, G have no common factors, $R := \text{Res}(F, G)$ the resultant of F and G is a nonzero integer. Also, there are $f_1, g_1, f_2, g_2 \in \mathbb{Z}[x, y]$ homogeneous polynomials such that

$$f_1(x, y)F(x, y) + g_1(x, y)G(x, y) = Rx^{2d-1}$$

$$f_2(x, y)F(x, y) + g_2(x, y)G(x, y) = Ry^{2d-1}.$$

Suppose $\phi(\alpha) \in \mathbb{Z}$. Substituting $(x, y) = (a, b)$ in the previous equations we see, since $G(a, b)$ divides $F(a, b)$, that $G(a, b)$ divides Ra^{2d-1} and Rb^{2d-1} . As we choose $\frac{a}{b}$ in lowest terms, $G(a, b)$ divides R .

Thus we have that

$$\{\alpha \in \mathbb{Q} : \phi(\alpha) \in \mathbb{Z}\} \subseteq \bigcup_{D|R} \{\alpha \in \mathbb{Q} : G(a, b) = D\}. \quad (2.3)$$

It is important to note that R does not depend on a and b , instead R is dependant only on ϕ .

Finally, from Theorem 2.2.2 using $K = \mathbb{Q}$ and $S = \{\infty\}$, for $D|R$ the set $\{\alpha \in \mathbb{Q} : G(a, b) = D\}$ is finite. As there are finitely many divisors for R , the set from the right side of (2.3) is finite and the theorem is true. ■

2.3 Arithmetic Dynamics

Our motivation to study Diophantine Approximation are some results that exist in the area of Arithmetic Dynamics. In particular, in the future we want to generalize the finiteness of S -units in the image of rational functions to finiteness of quasi- (S, ϵ) -units (Proposition 2.3.10). We will give the basic definitions and the results related to our problem.

This section is based in [Sil2].

Definition 2.3.1. [Sil2, Introduction] A **(discrete) dynamical system** consists of a set S and a function $\varphi: S \rightarrow S$ mapping the set S to itself. This self-mapping permits iteration

$$\phi^n = \underbrace{\phi \circ \phi \circ \cdots \circ \phi}_n.$$

By convention, ϕ^0 denotes the identity map on S .

Definition 2.3.2. For a given point $\alpha \in S$, the **(forward) orbit** of α is the set

$$\mathcal{O}_\phi(\alpha) = \{\phi^n(\alpha) : n \geq 0\}.$$

The point α is **periodic** if $\phi^n(\alpha) = \alpha$ for some $n \geq 1$. The smallest such n is called the **exact period** of α . The point α is **preperiodic** if some iterate $\phi^m(\alpha)$ is periodic. If a point is not preperiodic we say that it is a **wandering point**.

The sets of periodic and preperiodic points of ϕ in S are denoted respectively by

$$\text{Per}(\phi, S) = \{\alpha \in S : \phi^n(\alpha) = \alpha \text{ for some } n \geq 1\},$$

$$\text{PrePer}(\phi, S) = \{\alpha \in S : \phi^{m+n}(\alpha) = \phi^m(\alpha) \text{ for some } n \geq 1, m \geq 0\}.$$

As we are working with rational maps, we have some properties for the previous set.

Theorem 2.3.3 (Northcott). [Sil2, Theorem 3.12] *Let $\phi : \mathbb{P}^n \rightarrow \mathbb{P}^n$ be a morphism of degree $d \geq 2$ defined over a number field K . Then the set of preperiodic points $\text{PrePer}(\phi) \subseteq \mathbb{P}(\overline{K})$ is a set of bounded height. In particular,*

$$\text{PrePer}(\phi, \mathbb{P}^n(K)) = \text{PrePer}(\phi) \cap \mathbb{P}^n(K)$$

is a finite set.

As we saw in Theorem 1.1.24, $H(\phi(P))$ has a relation with $H(P)^d$. This is the motivation to define the canonical height.

Theorem 2.3.4. [Sil2, Theorem 3.20] *Let S be a set, $d > 1$ a real number and let $\phi: S \rightarrow S$ and $h: S \rightarrow \mathbb{R}$ be functions satisfying*

$$h(\phi(P)) = dh(P) + O(1) \quad \text{for all } P \in S.$$

Then the limit

$$\hat{h}(P) = \lim_{n \rightarrow \infty} \frac{1}{d^n} h(\phi^n(P))$$

exists and satisfies:

1. $\hat{h}(P) = h(P) + O(1)$.
2. $\hat{h}(\phi(P)) = d\hat{h}(P)$.

The function $\hat{h}: S \rightarrow \mathbb{R}$ is uniquely determined by the properties above.

Definition 2.3.5. Let $\phi: \mathbb{P}^n \rightarrow \mathbb{P}^n$ be a morphism of degree $d \geq 2$. The **canonical height function** (associated to ϕ) is the unique function

$$\hat{h}_\phi: \mathbb{P}^n(\overline{\mathbb{Q}}) \rightarrow \mathbb{R}$$

satisfying $\hat{h}_\phi(P) = h(P) + O(1)$ and $\hat{h}_\phi(\phi(P)) = d\hat{h}_\phi(P)$.

The canonical height provides a useful arithmetic characterization of the preperiodic points of ϕ .

Theorem 2.3.6. [Sil2, Theorem 3.22] Let $\phi: \mathbb{P}^n \rightarrow \mathbb{P}^n$ be a morphism of degree $d \geq 2$ defined over $\overline{\mathbb{Q}}$ and let $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Then

$$P \in \text{PrePer}(\phi) \quad \text{if and only if} \quad \hat{h}_\phi(P) = 0.$$

We are motivated by the following result from Silverman.

Theorem 2.3.7. [Sil2, Theorem 3.43] Let $\phi(z) \in \mathbb{Q}(z)$ be a rational map of degree $d \geq 2$ with the property that $\phi^2(z) \notin \mathbb{Q}[z]$. Let $\alpha \in \mathbb{Q}$ be a wandering point for ϕ . Then the orbit $\mathcal{O}_\phi(\alpha)$ contains only finitely many integer points.

In [Sil1, Theorem 2.2] Silverman generalizes this result to number fields and using S -integers instead of integers. It is natural to ask if the number of S -integral points of ϕ can be uniformly bounded. A work in this direction is given by Gunther and Hindes in [GH]. They proved the following

Theorem 2.3.8. [GH, Theorem 1.6 a.] Let $\phi(z) \in \overline{\mathbb{Q}}(z)$ be a rational function of degree at least two and let S be a finite set of places of \mathbb{Q} containing the archimedean one. Then if $\phi^2(z)$ is not a polynomial, there exists a constant $N = N(\phi, d, S)$ such that for every point $P \in \mathbb{P}^1(\overline{\mathbb{Q}}, d)$, we have $\#(\text{Orb}_\phi(P) \cap \mathcal{O}_S) \leq N$.

Remark 2.3.9. The number of S -integers in $\phi(K)$ cannot be bounded in terms of only K, S and $\deg \phi$. In [Sil1] Silverman shows the following example: Let $\phi(z) \in \mathbb{Q}(z)$ be any rational function and let $t \in \mathbb{Q}$ be any point whose orbit $\mathcal{O}_\phi(t)$ is infinite. For each n write $\phi^n(t) = \frac{a_n}{b_n}$ in lowest terms. Now choose an integer N and define $B = b_0 b_1 \cdots b_N$. (If some $b_i = 0$, we discard it). The function $\psi(z) = B\phi(z/B)$ then has the property that

$$\psi^n(Bt) = B\phi^n(t) = B\frac{a_n}{b_n} \in \mathbb{Z} \quad \text{for all} \quad 0 \leq n \leq N,$$

and then $\mathcal{O}_\psi(Bt)$ contains at least N integers points.

But [KLSTYZ] conjecture that, in the case of S -units, there is a bound depending only on $|S|$ and $\deg \phi$.

Conjecture 1. [KLSTYZ, Conjecture 1.1] *For any integers $s \geq 1$ and $d \geq 2$, there is a constant $C = C(s, d)$ such that for any number field K , s -element set S of places of K including the archimedean ones and degree- d rational function $\phi(z) \in K(z)$ which is not a d -th power in $\overline{K}(z)$, we have*

$$|\phi(K) \cap R_S^*| \leq C.$$

In [KLSTYZ] they prove the conjecture in the case of $\phi(z)$ restricted to certain classes of rational functions. However, the conjecture would be true if we allowed the constant C depend on K, S and ϕ instead on d and s . For this they use

Proposition 2.3.10. [KLSTYZ, Proposition 1.5] *Let K be a number field, let S be a finite set of places of K including the archimedean and let $\phi(z) \in K(z)$ be any rational function. If $|\phi^{-1}(\{0, \infty\})| \neq 2$ then $\phi(K) \cap R_S^*$ is finite.*

For this last Proposition, they apply Siegel's Theorem 2.2.3 over the function

$$\psi(z) = \phi(z) + \frac{1}{\phi(z)}$$

and conclude using the fact that

$$\phi(R_S^*) \subseteq \psi(R_S).$$

Thus, our motivation to prove a version for quasi-integers of Siegel's Theorem is generalizing Proposition 2.3.10 to quasi-units.

Chapter 3

Main Theorem

3.1 Modified Thue's Theorem

In the first place we recall a relation between the roots and coefficients of a polynomial:

Lemma 3.1.1 (Lagrange). *Let $p(x) = a_0 + a_1x + \cdots + a_nx^n$ be a polynomial with $a_i \in \mathbb{R}$ and $a_n \neq 0$. Then, every complex root of $p(x)$ is bounded by*

$$\max \left\{ 1, \sum_{i=0}^{n-1} \left| \frac{a_i}{a_n} \right| \right\}.$$

Searching for an analogue of Thue's Theorem in the case of quasi-integral points we prove:

Theorem 3.1.2 (Modified Thue's Theorem). *Let $G \in \mathbb{Z}[x, y]$ be a homogeneous function having at least 3 different factors over \mathbb{C} . There is a constant $c(d) > 0$ depending only on $d := \deg G$ such that for every $0 \leq \gamma < c(d)$ the inequality*

$$|G(x, y)| \leq \max\{|x|, |y|\}^\gamma$$

has at most finitely many solutions in \mathbb{Z}^2 .

Proof. The case when G is square-free implies the general case in the following way: We can assume that the constant $c(d)$ is decreasing as the degree grows. Suppose G is not square-free, then we can write $G(x, y) = G_1(x, y)G_2(x, y)$ where $G_1, G_2 \in \mathbb{Z}[x, y]$ and G_1 has the same roots as G but is square-free. Then $d_1 = \deg G_1 < d$ and $c(d) < c(d_1)$.

If $(a, b) \in \mathbb{Z}$ are such that $|G(a, b)| \leq \max\{|a|, |b|\}^\gamma$ for some $0 < \gamma \leq c(d)$, then

$$|G_1(a, b)| \leq |G(a, b)| \leq \max\{|a|, |b|\}^\gamma.$$

As $\gamma \leq c(d) < c(d_1)$, the Theorem applied to $G_1(x, y)$ implies there are finitely many $(a, b) \in \mathbb{Z}$ such that $|G(a, b)| \leq \max\{|a|, |b|\}^\gamma$.

From now on suppose that G is square-free. In the first place, we will study the case when G is reducible over $\mathbb{Z}[x, y]$. That is $G(x, y) = U(x, y)V(x, y)$ for some distinct $U, V \in \mathbb{Z}[x, y]$. As we are assuming G square-free, U and V have no common factors in $\mathbb{Z}[x, y]$. We shall prove that the system

$$U(x, y) = A \tag{3.1}$$

$$V(x, y) = B \tag{3.2}$$

$$|AB| \leq \max\{|x|, |y|\}^\gamma \tag{3.3}$$

with $A, B \in \mathbb{Z}$ has at most finite solutions in \mathbb{Z}^2 .

Notice that $U - A, V - B$ are not homogeneous, so we use the resultant of $U - A, V - B$ with respect to y denoted $\text{Res}_y(U - A, V - B) \in \mathbb{Z}[x]$ as we defined in 1.2.3.

Recall from Proposition 1.2.7 that if $(a, b) \in \mathbb{Z}^2$ is a solution of (3.1) and (3.2), then a is such that $\text{Res}_y(U - A, V - B)(a) = 0$. By Lemma 3.1.1, if

$$\text{Res}_y(U - A, V - B) = a_n x^n + \cdots + a_1 x + a_0,$$

then

$$|a| \leq \max \left\{ 1, \sum_{i=0}^{n-1} \left| \frac{a_i}{a_n} \right| \right\} \leq \max \left\{ 1, \sum_{i=0}^{n-1} |a_i| \right\} \leq \sum_{i=0}^{n-1} |a_i|. \tag{3.4}$$

As the resultant is the determinant of a matrix with the coefficients of $U - A, V - B$ as entries, its coefficients as a polynomial from $\mathbb{Z}[x]$ are determined by U, V (and then, G) and A, B . Even more, A appears in $\deg_y(U - A)$ entries and B appears in $\deg_y(V - B)$ entries. So, the power of A, B in the coefficients of $\text{Res}_y(U - A, V - B)$ is bounded by

$$\deg_y(U - A) + \deg_y(V - B) \leq d,$$

It follows that

$$|a| \leq C(U, V) \max\{|A|, |B|\}^d.$$

where $C(U, V)$ is a constant depending only on U and V .

Hence if $(a, b) \in \mathbb{Z}^2$ is a solution for the system (3.1) (3.2) (3.3), we have

$$|a| \leq C(U, V) \max\{|a|, |b|\}^{d\gamma}.$$

Using the fact that if $(a, b) \in \mathbb{Z}^2$ is a solution of (3.1) (3.2), then

$$\text{Res}_x(U - A, V - B)(b) = 0,$$

we conclude in an analogous way that

$$|b| \leq C'(U, V) \max\{|a|, |b|\}^{d\gamma}$$

where $C'(U, V)$ is a constant depending only on U and V .

Finally, if (a, b) is a solution of the system, then

$$\max\{|a|, |b|\} \leq \max\{C, C'\} \max\{|a|, |b|\}^{d\gamma}$$

which implies that

$$\max\{|a|, |b|\}^{1-d\gamma} \leq \max\{C, C'\}. \quad (3.5)$$

As a, b are integers, if $1 - d\gamma > 0$ then there are at most finitely many (a, b) that satisfy (3.5). For this case it is enough to take $c(d) \leq \frac{1}{d}$.

Now we will prove the case where G is irreducible over $\mathbb{Z}[x, y]$. By Gauss' Lemma, then G is irreducible over $\mathbb{Q}[x, y]$. So, factoring over $\mathbb{C}[x, y]$ we have

$$G(x, y) = A(x - \alpha_1 y)(x - \alpha_2 y) \cdots (x - \alpha_d y)$$

with $\alpha_i \neq \alpha_j$ for all $i \neq j$.

Notice that if we divide by y^d we have

$$\frac{G(x, y)}{y^d} = A \left(\frac{x}{y} - \alpha_1 \right) \cdots \left(\frac{x}{y} - \alpha_d \right).$$

Let us define $\delta := \frac{\min\{|\alpha_i - \alpha_j| : i \neq j\}}{2}$, then at most one α_i satisfies $\left| \frac{x}{y} - \alpha_i \right| < \delta$ for $\frac{x}{y} \in \mathbb{Q}$. So,

$$\left| \frac{G(x, y)}{y^d} \right| \geq A\delta^{d-1} \min_{1 \leq i \leq d} \left| \frac{x}{y} - \alpha_i \right|,$$

and then

$$\min_{1 \leq i \leq d} \left| \frac{x}{y} - \alpha_i \right| \leq \frac{|G(x, y)|}{A\delta^{d-1}|y|^d}.$$

On the other side, if we apply Roth's Theorem (2.2.1) for every α_j , then there exists some $k = k(1/4, \alpha_1, \dots, \alpha_d) > 0$ such that

$$\min_{1 \leq i \leq d} \left| \frac{x}{y} - \alpha_i \right| \geq \frac{k}{|y|^{2+1/4}}.$$

Suppose $|G(a, b)| \leq \max\{|a|, |b|\}^\gamma$, then using both inequalities above we have:

$$\frac{k}{|b|^{2+1/4}} \leq \min_{1 \leq i \leq d} \left| \frac{a}{b} - \alpha_i \right| \leq \frac{|G(a, b)|}{A\delta^{d-1}|b|^d} \leq \frac{\max\{|a|, |b|\}^\gamma}{A\delta^{d-1}|b|^d}.$$

From this we can conclude that

$$|b|^{d-2.25} \leq \frac{1}{A\delta^{d-1}k} \max\{|a|, |b|\}^\gamma. \quad (3.6)$$

We obtain a similar bound for $|a|$ writing

$$\frac{G(x, y)}{x^d} = B \left(\frac{y}{x} - \beta_1 \right) \cdots \left(\frac{y}{x} - \beta_d \right)$$

and using the constant κ' from Roth's theorem (2.2.1) over $\beta_1 \dots \beta_d$

$$|a|^{d-2.25} \leq \frac{1}{B\delta^{d-1}\kappa'} \max\{|a|, |b|\}^\gamma. \quad (3.7)$$

And then, using (3.6) and (3.7) we obtain

$$\max\{|a|, |b|\}^{d-2.25} \leq C \max\{|a|, |b|\}^\gamma,$$

where $C = \max\{\frac{1}{A\delta^{d-1}k}, \frac{1}{B\delta^{d-1}\kappa'}\}$ depends only on G (specifically on G 's roots).

For this case, we conclude that if $|G(a, b)| \leq \max\{|a|, |b|\}^\gamma$, then

$$\max\{|a|, |b|\}^{d-2.25-\gamma} \leq C.$$

So, if $\gamma < d - 2.25$ then there are finitely many integers $a, b \in \mathbb{Z}$ such that

$$|G(a, b)| \leq \max\{|a|, |b|\}^\gamma.$$

Finally, it is enough to consider $c(d) = \min\{\frac{1}{d}, d - 2.25\}$. Then, in both of the cases, if $0 \leq \gamma < c(d)$ we have only finitely many solutions $(a, b) \in \mathbb{Z}^2$ for the inequality

$$|G(x, y)| \leq \max\{|x|, |y|\}^\gamma.$$

■

3.2 Siegel for quasi-integral points

Theorem 3.2.1 (Siegel for quasi-integral points). *Let $\phi(z) \in \mathbb{Q}(z)$ be a rational function of degree d with at least three distinct poles in $\mathbb{P}^1(\mathbb{C})$. There exists a constant $c(d) > 0$ depending only on d such that for every $0 \leq r < c(d)$,*

$$\{\alpha \in \mathbb{Q} : \phi(\alpha) \text{ is } r\text{-quasi-integral}\}$$

is a finite set.

Proof. The proof is based on 2.2.3.

In the first place, we write $\phi = [F(x, y), G(x, y)]$ where $F(x, y), G(x, y) \in \mathbb{Z}[x, y]$ are homogeneous polynomials of degree d with no common factors. So, for any $\alpha = \frac{a}{b} \in \mathbb{Q}$ written in lowest terms, we have

$$\phi(\alpha) = \frac{F(a, b)}{G(a, b)}.$$

We denote $d' = d'(a, b) := \gcd(F(a, b), G(a, b))$. Note that if we write $\phi(\alpha)$ in lowest terms its denominator will be $\frac{G(a, b)}{d'}$. Suppose $\phi(\alpha)$ is r -quasi-integral, then

$$|G(a, b)| \leq d' H(\phi(\alpha))^r. \tag{3.8}$$

Recall that F, G have no common factors, so $R := \text{Res}(F, G)$ the resultant of F and G is a nonzero integer. In Proposition 1.2.1 it was proven that there are $f_1, g_1, f_2, g_2 \in \mathbb{Z}[x, y]$ homogeneous polynomials such that

$$f_1(x, y)F(x, y) + g_1(x, y)G(x, y) = Rx^{2d-1}$$

$$f_2(x, y)F(x, y) + g_2(x, y)G(x, y) = Ry^{2d-1}.$$

By definition, d' divides $F(a, b)$ and $G(a, b)$. Substituting $(x, y) = (a, b)$ in the previous equations we see that d' divides Ra^{2d-1} and Rb^{2d-1} . Since we chose $\frac{a}{b}$ in lowest terms, d' divides R .

By [HinSil, Theorem 3.11] there is a constant $C > 0$, depending on ϕ , such that

$$H(\phi(P)) \leq CH(P) \quad \text{for all } P \in \mathbb{P}^1(\mathbb{Q}).$$

Using the previous inequality and (3.8) we have

$$\{\alpha \in \mathbb{Q} : \phi(\alpha) \text{ is } r\text{-quasi-integral}\} \subseteq \bigcup_{D|R} \{\alpha \in \mathbb{Q} : |G(a, b)| \leq DC^r H(\alpha)^{dr}\}. \quad (3.9)$$

It is important to note that C, R does not depend on a and b , instead they are only dependant on ϕ .

Finally, it is enough to prove that for $D|R$ the set

$$\{\alpha \in \mathbb{Q} : |G(a, b)| \leq DC^r H(\alpha)^{dr}\}$$

is finite. For this, we will divide this set in two and prove that each part is finite:

- If $DC^r \leq H(\alpha)^{dr}$, then $|G(a, b)| \leq H(\alpha)^{2dr}$ and the Modified Thue's theorem (3.1.2) implies that there exists some $c(d) > 0$ depending only on $\deg G$ such that if $2dr < c(d)$ then this inequality has at most finitely many solutions in \mathbb{Z}^2 .
- From Northcott's property (1.1.21) there exist only finitely many $\alpha \in \mathbb{Q}$ such that $H(\alpha)^{dr} \leq DC^r$.

So, we conclude that for every $r < \frac{c(d)}{2d}$ and each $D|R$ the set

$$\{\alpha \in \mathbb{Q} : |G(a, b)| \leq DC^r H(\alpha)^{dr}\}$$

is finite. As there are finitely many divisors for R , the set from the right side of (3.9) is finite and the theorem is true. ■

Bibliography

- [CLO] D. Cox, J. Little, and D. O’Shea. *Ideals, varieties, and algorithms*. An introduction to computational algebraic geometry and commutative algebra. Third edition. Undergraduate Texts in Mathematics. Springer, New York, 2007.
- [GH] J. Gunther and W. Hindes. *Integral points of bounded degree on the projective line and in dynamical orbits*. Proc. Amer. Math. Soc. 145 (2017), no. 12, 5087–5096.
- [HinSil] M. Hindry and J. H. Silverman. *Diophantine geometry. An introduction*. Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000.
- [HsiaSil] L. Hsia and J. H. Silverman. *A quantitative estimate for quasiintegral points in orbits*. Pacific J. Math. 249 (2011), no. 2, 321–342.
- [KLSTYZ] H. Krieger, A. Levin, Z. Scherr, T. Tucker, Y. Yasufuku, and M. E. Zieve. *Uniform boundedness of S -units in arithmetic dynamics*, Pacific J. Math. 274 (2015), 97–106.
- [Neu] J. Neukirch. *Algebraic number theory*. Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin, 1999.
- [Sil1] J. H. Silverman. *Integer points, Diophantine approximation, and iteration of rational maps*. Duke Math. J. 71 (1993), no. 3, 793–829.
- [Sil2] J. H. Silverman. *The arithmetic of dynamical systems*. Graduate Texts in Mathematics, 241. Springer, New York, 2007.