Heights on Projective Spaces

Anco Moritz

advisor: dr. C. Salgado Guimaraes de Silva

9th June 2010

Mathematical Institute, Leiden University

Contents

Introduction

Dynamics and number theory long were quite dinstinct fields of mathematics. Recently, however, progress has been made in the application of number theory to dynamics. This text seeks to elucidate a small bit of this progress.
The focus will be on the special case of discrete dynamical systems, which consist of a set X associated with a map $\phi : X \to X$. As in this text we will mainly consider $X = \mathbb{P}^n(\mathbb{Q})$, the first section serves as an introduction to projective geometry. To provide the reader with some intuition, it starts out with $\mathbb{P}^1(\mathbb{C})$ and eventually switches attention to $\mathbb{P}^n(\mathbb{Q})$.
The second section introduces the basic notions of discrete dynamics.
In the third section, 'height functions' are defined. These are functions of the form $h : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}$, and they serve as the main tool in applying number theory to dynamics. As we restrict attention to projective spaces over $\mathbb{Q}$, their definitions can remain quite simple; when working over an arbitrary number field K, one runs into the problem that the ring of integers of K may not be a principal ideal domain, making the definition of h substantially more complicated. For this, refer to [1].
After having defined them, some important properties of the height functions are derived. Section 4 then utilizes these properties to quickly derive some interesting theorems relating arithmetic to discrete dynamical systems.

1 Some projective geometry

Definition 1.1. Let V be a vector space. The *projective space over* V, denoted $\mathbb{P}(V)$, is the set of 1-dimensional subspaces of V.

Remark 1.2. When in this text we speak of a vector space, we mean a finite-dimensional vector space.

Example 1.3. Let $V = \mathbb{R}^2$. Then $\mathbb{P}(V) = \mathbb{P}(\mathbb{R}^2)$ is the set of lines through the origin. Note the following: almost every $p \in \mathbb{P}(\mathbb{R}^2)$, being a subset of $\mathbb{R}^2$, has exactly one point in common with the line $\ell := \{(x, y) \in \mathbb{R}^2 \mid y = 1\}$, the only exception being $\infty := \{(x, y) \in \mathbb{R}^2 \mid y = 0\} \in \mathbb{P}(\mathbb{R}^2)$. One can thus identify $\mathbb{P}(\mathbb{R}^2)\backslash\{\infty\}$ with ℓ, which, in turn, is just a copy of $\mathbb{R}$. This leads to an identification of $\mathbb{P}(\mathbb{R}^2)$ with $\mathbb{R} \cup \{\infty\}$.

Example 1.4. For $V = \mathbb{C}^2$, we see analogously that almost every $p \in \mathbb{P}(\mathbb{C}^2)$ has exactly one point $x \in \mathbb{C}^2$ in common with $\ell := \{(w, z) \in \mathbb{C}^2 \mid z = 1\}$. Namely, if $p = \{\lambda(p_1, p_2) \mid \lambda \in \mathbb{C}\}$ for some $p_1, p_2 \in \mathbb{C}\backslash\{0\}$, then $x = (\frac{p_1}{p_2}, 1)$. The unique exception is $\infty := \{(w, z) \in \mathbb{C}^2 \mid z = 0\} \in \mathbb{P}(\mathbb{C}^2)$. Since ℓ is a copy of $\mathbb{C}$, this observation gives rise to an identification of $\mathbb{P}(\mathbb{C}^2)$ with $\mathbb{C} \cup \{\infty\}$.

Definition 1.5. Let V be an n-dimensional vector space. The *dimension* of $\mathbb{P}(V)$ is $n - 1$.

Notation 1.6. Motivated by the preceding definition, if K is a number field, $\mathbb{P}(K^{n+1})$ is often denoted as $\mathbb{P}^n(K)$. If $n = 1$ and K equals $\mathbb{R}$ or $\mathbb{C}$, we respectively speak about the *real projective line* and the *complex projective line*.

As we have seen, the complex projective line can be identified with $\mathbb{C}\cup\{\infty\}$. In turn, the complex plane can be identified with the unit sphere S^2 without its north pole N. To see this, we identify $\mathbb{C}$ with $\{(x, y, z) \in \mathbb{R}^3 \mid z = 0\}$, set $S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$ and $N = (0, 0, 1) \in \mathbb{R}^3$. For an arbitrary point $z \in S^2\backslash\{N\}$, the line through N and z will cut $\mathbb{C}$ in exactly one point z^*. This way of relating points to each other is called *stereographic projection* (see figure 1) and it yields the asserted identification. We can go a step further by sending N to the point $\infty \in \mathbb{C} \cup \{\infty\}$, giving rise to a bijection $f : S^2 \to \mathbb{P}^1(\mathbb{C})$.

Definition 1.7. Let $S^2 \subset \mathbb{R}^3$ be the unit sphere, let $|\cdot|$ denote the Euclidean norm on $\mathbb{R}^3$, let f be as above and let $g := f^{-1}$. The *chordal metric* is the metric ρ on $\mathbb{P}^1(\mathbb{C})$ given by $\rho(x, y) = |g(x) - g(y)|$.

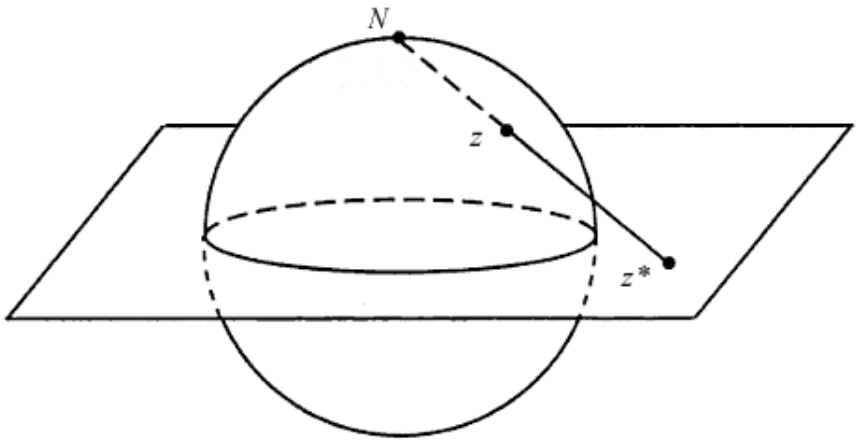

Figure 1: stereographic projection

Theorem 1.8. Identify $\mathbb{P}^1(\mathbb{C})$ with $\mathbb{C} \cup \{\infty\}$ as in example 1.3 and let $|\cdot|$ denote the Euclidean norm on $\mathbb{C}$. The chordal metric is given by

$$\rho(x,y) = \begin{cases} \frac{2|x-y|}{\sqrt{|x|^2+1}\sqrt{|y|^2+1}} & \text{if } x \neq \infty \neq y \\ \frac{2}{\sqrt{|x|^2+1}} & \text{if } x \neq \infty = y \end{cases}$$

Proof. Let g be as in definition 1.7 and let $a = a_1 + a_2 i \in \mathbb{C}$. In order to calculate $g(a)$, let us identify a with $(a_1, a_2, 0) \in \mathbb{R}^3$. Now the image of a under g is the unique intersection point of $S^2 = \{(x,y,z) \in \mathbb{R}^3 \mid x^2+y^2+z^2 = 1\}$ and $\ell = \{(1-\lambda)(0,0,1) + \lambda(a_1,a_2,0) \mid \lambda \in \mathbb{R}_{>0}\}$. Hence we solve for λ the equation

$$(\lambda a_1)^2 + (\lambda a_2)^2 + (1-\lambda)^2 = 1,$$

finding

$$\lambda = \frac{2}{a_1^2 + a_2^2 + 1},$$

from which it follows that

$$g(a) = \left(\frac{2a_1}{a_1^2+a_2^2+1}, \frac{2a_2}{a_1^2+a_2^2+1}, \frac{a_1^2+a_2^2-1}{a_1^2+a_2^2+1} \right). \tag{1}$$

Next, observe that if $a = (a_1, a_2, a_3)$ and $b = (b_1, b_2, b_3)$ are points on S^2, then

$$\begin{aligned} |a-b| &= \sqrt{(a_1-b_1)^2+(a_2-b_2)^2+(a_3-b_3)^2} \\ &= \sqrt{(a_1^2+a_2^2+a_3^2)+(b_1^2+b_2^2+b_3^2)-2a_1b_1-2a_2b_2-2a_3b_3} \\ &= \sqrt{2-2a_1b_1-2a_2b_2-2a_3b_3}. \end{aligned} \tag{2}$$

Now let $x = x_1 + x_2 i$, $y = y_1 + y_2 i \in \mathbb{C}$. We identify these points with $(x_1, x_2, 0)$ and $(y_1, y_2, 0) \in \mathbb{R}^3$ respectively. Let $g(x)_i$ and $g(y)_i$ denote the ith coordinates of the images of x and y under g. We know from (2) that

$$|g(x) - g(y)| = \sqrt{2 - 2g(x)_1 g(y)_1 - 2g(x)_2 g(y)_2 - 2g(x)_3 g(y)_3}, \tag{3}$$

and it follows from (1) that this equals

$$\sqrt{2 - \frac{2 \cdot 2x_1 \cdot 2y_1 - 2 \cdot 2x_2 \cdot 2y_2 - 2 \cdot (x_1^2 + x_2^2 - 1) \cdot (y_1^2 + y_2^2 - 1)}{(x_1^2 + x_2^2 + 1) \cdot (y_1^2 + y_2^2 + 1)}}$$

$$\begin{aligned} &= \sqrt{\frac{4(x_1^2+x_2^2)+4(y_1+y_2)-8x_1y_1-8x_2y_2}{(x_1^2+x_2^2+1)(y_1^2+y_2^2+1)}} \\ &= \sqrt{\frac{4((x_1-y_1)^2+(x_2-y_2)^2)}{(x_1^2+x_2^2+1)(y_1^2+y_2^2+1)}} \\ &= \frac{2\sqrt{(x_1-y_1)^2+(x_2-y_2)^2}}{\sqrt{x_1^2+x_2^2+1}\sqrt{y_1^2+y_2^2+1}} = \frac{2|x-y|}{\sqrt{|x|^2+1}\sqrt{|y|^2+1}}. \end{aligned}$$

If y is the point at infinity, we know that $g(y) = (0, 0, 1)$. Hence in this case, (3) equals

$$\begin{aligned} |g(x) - g(y)| &= \sqrt{2 - 2g(x)_1 \cdot 0 - 2g(x)_2 \cdot 0 - 2g(x)_3 \cdot 1} \\ &= \sqrt{2 - 2g(x)_3} \\ &= \sqrt{2 - 2\frac{x_1^2 + x_2^2 - 1}{x_1^2 + x_2^2 + 1}} \\ &= \sqrt{\frac{4}{x_1^2 + x_2^2 + 1}} = \frac{2}{\sqrt{|x|^2 + 1}}. \end{aligned}$$

□

The following will play an important role in our study of height functions.

Definition 1.9. A *rational function on* $\mathbb{C}$ is an ordered pair (f, g) of polynomials $f, g \in \mathbb{C}[X]$ satisfying exactly one of the following conditions:

(1) $f = 0$ and $g = 1$.

(2) f is monic and f and g have no common factors.

Definition 1.10. A *rational map* on $\mathbb{P}^1(\mathbb{C})$ is a map $\phi : \mathbb{C} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$, denoted $\mathbb{C} \cup \{\infty\} \dashrightarrow \mathbb{C} \cup \{\infty\}$, satisfying the following conditions:

(1) There is a rational function (f, g) on $\mathbb{C}$ such that for every $z \in \mathbb{C}$ with $g(z) \neq 0$: $\phi(z) = f(z)/g(z)$.

(2) For every $z \in \mathbb{C}$ with $g(z) = 0 : \phi(z) = \infty$.

(3) $\phi(\infty) = \lim_{z \to \infty} f(z)/g(z)$, where the limit function is defined with respect to the chordal metric.

Note that for a given rational map ϕ on $\mathbb{P}^1(\mathbb{C})$, the rational function satisfying condition (1) is unique. This justifies the following definition.

Definition 1.11. Let ϕ be a rational map on $\mathbb{P}^1(\mathbb{C})$ with associated rational function (f, g). The *degree of* ϕ is $\deg(\phi) = \max\{\deg(f), \deg(g)\}$.

For V an n-dimensional vector space with scalar field K, we can define an equivalence relation $\sim$ on $V^* := V \backslash \{0\}$ as follows:

$$x \sim y \iff \exists \lambda \in K : x = \lambda y$$

Note that the map $\phi : V^*/\sim \to \mathbb{P}(V)$, given by $p \mapsto p \cup \{0\}$, is a bijection. This is another way of looking at $\mathbb{P}(V)$, and instead of $\phi(p) = q$ we will write $p = q$. We have lain the ground for the following definition.

Definition 1.12. Let V, n, K and $\sim$ be as above and fix a basis B for V. Let $p \in V^*$ and let $(p_1, p_2, ..., p_n)$ be the coordinates of p relative to B. We denote the equivalence class of p relative to $\sim$ by $(p_1 : p_2 : ... : p_n)$. The scalars $(p_1, p_2, ..., p_n) \in K^n \backslash \{0\}$ are called *homogeneous coordinates* of $(p_1 : p_2 : ... : p_n) \in \mathbb{P}(V)$.

Note that one cannot talk about homogenous coordinates of a point $p \in \mathbb{P}(V)$ without having chosen a basis for V. Note also that homogeneous coordinates of p are not unique: $(p_1 : p_2 : ...p_n) = (\lambda p_1 : \lambda p_2 : ... : \lambda p_n)$ for every $\lambda \in K^*$.

Definition 1.13. Let $\mathbb{P}(V)$ be an n-dimensional projective space with a chosen basis for V and let $p = (p_0 : p_1 : ... : p_n) \in \mathbb{P}(V)$ be such that $p_n \neq 0$. *Affine coordinates of* p are scalars $(a_0, a_1, ..., a_{n-1})$ for which $p = (a_o : a_1 : ... : a_{n-1} : 1)$. We will write $p = (a_0, a_1, ..., a_{n-1})$.

Lemma 1.14. Let $\phi : \mathbb{P}^1(\mathbb{C}) \dashrightarrow \mathbb{P}^1(\mathbb{C})$ be a rational map of degree d with associated rational function (f, g). For $F, G \in \mathbb{C}[X, Y]$ defined by $F = Y^d f(X/Y)$ and $G = Y^d g(X/Y)$, the map ϕ can be writen as $(x : y) \mapsto (F(x, y) : G(x, y))$.

Proof. We wish to define

$$\pi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$$
$$(x : y) \mapsto (F(x, y) : G(x, y))$$

and prove that $\phi(p) = \pi(p)$ for every $p \in \mathbb{P}^1(\mathbb{C})$. We must first, however, verify that π is actually a map, i.e., that π is well defined and that $F(x, y) = G(x, y) = 0$ if and only if $x = y = 0$.
Let us begin with the latter. Observing that F and G have no constant terms, the equality $F(0, 0) = G(0, 0) = 0$ follows immediately. Now let $(x, y) \in \mathbb{C}^2$ be such that $F(x, y) = G(x, y) = 0$. Suppose $y \neq 0$. Then

$$f(\tfrac{x}{y}) = \frac{F(x, y)}{y^d} = 0 = \frac{G(x, y)}{y^d} = g(\tfrac{x}{y}),$$

from which it follows that f and g share a factor $(X - \frac{x}{y})$, which, by definition 1.9, is a contradiction. We conclude $y = 0$. Now since at least one of the polynomials F and G have exactly one monomial with no factor Y, it follows from $F(x, 0) = G(x, 0) = 0$ that $x = 0$.
For the well definedness of π, we observe that F and G have the property that for any $x, y, z \in \mathbb{C}$:

$$F(zx, zy) = z^d F(x, y) \qquad \text{and} \qquad G(zx, zy) = z^d G(x, y).$$

Now let $p = (x : y) \neq (1 : 0)$ be such that $g(\frac{x}{y}) \neq 0$. Then $\phi(p) = f(\frac{x}{y})/g(\frac{x}{y}) = (f(\frac{x}{y})/g(\frac{x}{y}) : 1) = (f(\frac{x}{y}) : g(\frac{x}{y})) = (F(x, y) : G(x, y))$, as desired.
Next, let $p = (x : y) \neq (1 : 0)$ be such that $g(\frac{x}{y}) = 0$. Then $G(x, y) = y^d g(\frac{x}{y}) = 0$ and $F(x, y) = y^d f(\frac{x}{y}) \neq 0$, so $\pi(x : y) = (1 : 0) = \infty = \phi(p)$.
Now let us look at the point $(1 : 0)$. If $\deg(g) < \deg(f)$, then every monomial of G has a factor Y, so $G(1, 0) = 0$. In F, on the other hand, there is precisely one monomial with no factor Y, so $F(1, 0) \neq 0$ and thus $\pi(1 : 0) = (1 : 0) = \infty = \lim_{z\to\infty} f(z)/g(z)$. If $\deg(g) = \deg(f)$, both f and g have exactly one monomial with no factor Y, so that $\pi(1 : 0) = (a_f : a_g) = \frac{a_f}{a_g} = \lim_{z\to\infty} f(z)/g(z)$, where a_f and a_g denote the leading coefficients of f and g respectively. Lastly, if $\deg(g) > \deg(f)$, we see that $\pi(1 : 0) = (0 : 1) = 0 = \lim_{z\to\infty} f(z)/g(z)$. □

As the main focus of this text is to derive some interesting theorems ragarding maps from $\mathbb{P}^n(\mathbb{Q})$ to itself, we shift attention from $\mathbb{P}^1(\mathbb{C})$ to $\mathbb{P}^n(K)$, where K is a number field.

Consider F and G as defined in the above lemma. The property $F(zx, zy) = z^d F(x, y)$ and $G(zx, zy) = z^d G(x, y)$ from the proof is an important one, which can be defined rigorously for polynomials over arbitrary number fields in any number of variables. For this, we will need to have a notion of *degree* for such polynomials.

Definitions 1.15. Let K be a number field.

(1) For $f = a\prod_i X_i^{a_i} \in K[X_1, ..., X_n]$ a monomial in n variables, the *degree of* f is $\deg(f) = \sum_i a_i$.

(2) For $\{f_1, ..., f_m\} \subset K[X_1, ..., X_n]$ a finite set of monomials and $g = \sum_i b_i f_i \in K[X_1, ..., X_n]$ a polynomial, the *degree of* g is $\deg(g) = \max_i(\deg(f_i))$.

Definition 1.16. Let K be a number field and let $\bar{X}$ denote a finite sequence of n variables. A polynomial $F \in K[\bar{X}]$ of degree d is called *homogeneous* if $F(\lambda\bar{X}) = \lambda^d F(\bar{X})$ for every $\lambda \in K$.

Example 1.17. Let K be a number field. The following are homogeneous polynomials in $K[X, Y, Z]$ of degree 1, 4 and 7 respectively:

- X
- $X^3Y - X^2Y^2$
- $XYZ^5 + XY^6 + Y^7$

Inspired by lemma 1.14, we now give a definition of rational maps over number fields and higher dimensions.

Definition 1.18. Let K be a number field, let $m, n \geq 1$ and let $U \subseteq \mathbb{P}^n(K)$ be open[1] and nonempty. A *rational map* is a map

$$\phi : U \to \mathbb{P}^m(K)$$
$$x = (x_0 : x_1 : ... : x_n) \mapsto (F_0(x) : F_1(x) : ... : F_m(x))$$

for homogeneous polynomials $F_0, F_1, ..., F_m$ of equal degree d for which there is no factor $h \in K[X_0, ..., X_n]$ dividing every $F_j \in \{F_1, ..., F_m\}$. The *degree of* ϕ is $\deg(\phi) = d$. Rational maps are denoted as $U \dashrightarrow \mathbb{P}^m(K)$.

Definition 1.19. Let K and ϕ be as in definition 1.17 and let $\bar{K}$ denote the algebraic closure of K. We say that ϕ is *defined at* $x \in \mathbb{P}^m(\bar{K})$ if there is an $i \in \{0, 1, ..., n\}$ such that $F_i(x) \neq 0$.

[1] According to the Zariski topology: see appendix A.

Definition 1.20. Let K and ϕ be as in definition 1.17 and let $\bar{K}$ denote the algebraic closure of K. We call ϕ a *morphism* if ϕ is defined at every $x \in \mathbb{P}^m(\bar{K})$.

Example 1.21. Let K be any number field and let $F_0 = X^2$, $F_1 = Y^2$, $F_2 = Z^2 \in K[X, Y, Z]$. Since F_0, F_1 and F_2 have no common factors and the only common root of F_0, F_1 and F_2 in $\bar{K}^3$ is (0,0,0), the map

$$\begin{gathered}\mathbb{P}^2(K) \dashrightarrow \mathbb{P}^2(K) \\ (x : y : z) \mapsto (F_0(x, y, z) : F_1(x, y, z) : F_2(x, y, z))\end{gathered}$$

is a morphism.

Example 1.22. Let $F_0 = X^2 + Y^2$, $F_1 = X^2 + Z^2$, $F_2 = X^2 + YZ$. Since F_0, F_1 and F_2 have no common factors in $\mathbb{Q}[X, Y, Z]$, the map

$$\begin{gathered}\mathbb{P}^2(\mathbb{Q}) \dashrightarrow \mathbb{P}^2(\mathbb{Q}) \\ (x : y : z) \mapsto (F_0(x, y, z) : F_1(x, y, z) : F_2(x, y, z))\end{gathered}$$

is a rational map. It is not a morphism, since $(i, 1, 1) \in \bar{\mathbb{Q}}^3$ is a common root of F_0, F_1 and F_2.

Example 1.23. Let $F = X^4 + Y^4$, $G = X^4$. Then F and G have no common factors in $\mathbb{Q}[X, Y]$. They also have no common roots in $\bar{\mathbb{Q}}^2$, so consequently

$$\begin{gathered}\mathbb{P}^1(\mathbb{Q}) \dashrightarrow \mathbb{P}^1(\mathbb{Q}) \\ (x : y) \mapsto (F(x, y) : G(x, y))\end{gathered}$$

is a morphism. This is not a coincidence.

Theorem 1.24. Let $U \subseteq \mathbb{P}^1(\bar{\mathbb{Q}})$ and let F and $G \in \mathbb{Q}[X, Y]$ be homogeneous polynomials such that

$$\begin{gathered}\phi : U \dashrightarrow \mathbb{P}^1(\bar{\mathbb{Q}}) \\ (x : y) \mapsto (F(x, y) : G(x, y))\end{gathered}$$

is a rational map. Then ϕ is a morphism.

Proof. We need to show that F and G have no common roots in $\bar{\mathbb{Q}}^2 \backslash \{(0, 0)\}$. Suppose therefore that they do: let $F(a, b) = G(a, b) = 0$ for some $a, b \in \bar{\mathbb{Q}}$ not both 0. Assume $b \neq 0$. First, we define polynomials $f, g \in \mathbb{Q}[X]$ by $f = F(X, 1)$ and $g = G(X, 1)$. Observe that

$$f(X/Y) = \sum_{i=0}^{d} a_i \frac{X^i}{Y^i} = \frac{\sum_{i=0}^{d} a_i X^i Y^{d-i}}{Y^d} = \frac{F(X, Y)}{Y^d}. \tag{4}$$

Now since F is homogeneous, we see that

$$f(\tfrac{a}{b}) = F(\tfrac{a}{b}, 1) = F(b^{-1}a, b^{-1}b) = b^{-d}F(a,b) = b^{-d} \cdot 0 = 0,$$

and analogously, we see $g(\frac{a}{b}) = 0$. This means the minimal polynomial $h \in \mathbb{Q}[X]$ of $\frac{a}{b} \in \bar{\mathbb{Q}}$ is a divisor of both f and g:

$$f = h \cdot f' \qquad \text{and} \qquad g = h \cdot g'$$

for some $f', g' \in \mathbb{Q}[X]$. Let $e = \deg(h)$. By (4):

$$\begin{aligned} F(X,Y) &= Y^d \cdot f(X/Y) \\ &= Y^d \cdot h(X/Y) f'(X/Y) \\ &= Y^e h(X/Y) \cdot Y^{d-e} f'(X/Y), \end{aligned}$$

and analogously we see $G(X,Y) = Y^e h(X/Y) \cdot Y^{d-e} g'(X/Y)$. Thus F and G share a factor $Y^e h(X/Y) \in \mathbb{Q}[X,Y]$.
Now suppose $F(a,0) = G(a,0) = 0$ for some $a \in \bar{\mathbb{Q}} \backslash \{0\}$. Then

$$0 = F(a,0) = \sum_{i=0}^{d} a_i a^i 0^{d-i} = a_d \cdot a^d,$$

so $a_d = 0$. The same reasoning shows that $b_d = 0$. Thus

$$F = \sum_{i=0}^{d-1} a_i X^i Y^{d-i} \quad \text{and} \quad G = \sum_{i=0}^{d-1} b_i X^i Y^{d-i},$$

so F and G have a common factor Y.
We conclude that if F and G have a common root, then they have a common factor, which contradicts the assumption of ϕ being a rational map. $\square$

2 Discrete dynamical systems

Definition 2.1. A *discrete dynamical system* is a set X associated with a map $\phi : X \to X$. Notation: (X, ϕ).

Definition 2.2. Let (X, ϕ) be a discrete dynamical system. A point $x \in X$ is called *periodic under* ϕ if there is an $n \geq 1$ such that $\phi^n(x) = x$. The set of periodic points under ϕ is denoted by $\mathrm{Per}(\phi)$.

Example 2.3. If X is a finite set, then for any $\phi : X \to X$ we have $\#\mathrm{Per}(\phi) \geq 1$. For suppose $\mathrm{Per}(\phi) = \emptyset$, then for any $x \in X$ and any $i, j \in \mathbb{Z}_{\geq 0}$ with $i \neq j$:

$$\phi^i(x) \neq \phi^j(x),$$

from which it would follow that X is infinite.

Example 2.4. Let $X = \mathbb{P}^1(\mathbb{Q})$ and let $\phi : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$ be given by $(x : y) \mapsto (x^2 : y^2)$. Suppose $(a : b) \in \mathbb{P}^1(\mathbb{Q})$ is periodic under ϕ, i.e., suppose $(a^{2n} : b^{2n}) = (a : b)$ for some $n \geq 1$. Then $a^{2n} = \lambda a$ and $b^{2n} = \lambda b$ for some $\lambda \in \mathbb{Q}$, so for $a \neq 0 \neq b$, we see $a^{2n-1} = \lambda = b^{2b-1}$ and thus $a = b$. It follows that (1:1) is the only rational non-zero periodic point under ϕ. A check shows that $(0 : 1)$ and $(1 : 0)$ are also periodic under ϕ, and we conclude

$$\mathrm{Per}(\phi) = \{(0 : 1), (1 : 1), (1 : 0)\}.$$

Definition 2.5. Let (X, ϕ) be a discrete dynamical system. A point $x \in X$ is called *preperiodic under* ϕ if there is an $m \geq 0$ such that $\phi^m(x)$ is periodic. The set of preperiodic points under ϕ is denoted by $\mathrm{PrePer}(\phi)$.

Note that for every discrete dynamical system (X, ϕ): $\mathrm{Per}(\phi) \subseteq \mathrm{PrePer}(\phi)$.

Example 2.6. If X is a finite set, then for any $\phi : X \to X$: $\mathrm{PrePer}(\phi) = X$. To see this, let $n = \#X$. For any $x \in X$, the set $\{x, \phi(x), \phi^2(x), ..., \phi^n(x)\}$ contains at most n elements. That is to say, there are $i, j \leq n$ with $i < j$ such that $\phi^i(x) = \phi^j(x)$. Thus x is preperiodic under ϕ.

Example 2.7. Let $X = \mathbb{Z}$ and let $\phi : \mathbb{Z} \to \mathbb{Z}$ be given by

$$\phi(n) = \begin{cases} n + 2 & \text{if } n \text{ is even} \\ |n| & \text{if } n \text{ is odd} \end{cases}$$

Then $n \in \mathbb{Z}$ is preperiodic under ϕ if and only if n is odd. If n is odd and $n > 0$, then n is periodic under ϕ.

Definition 2.8. Let (X, ϕ) be a discrete dynamical system and let $x \in X$. The *orbit of* x *under* ϕ is the set $\mathcal{O}_\phi(x) = \{\phi^n(x) \mid n \geq 0\}$.

Note that for every discrete dynamical system (X, ϕ) and every $x \in X$, the orbit of x under ϕ is finite if and only if x is preperiodic under ϕ.

Principal goal of discrete dynamics. For a given discrete dynamical system (X, ϕ), to classify its points according to their orbits.

In section 4, we will chase this goal for $X = \mathbb{P}^n(\mathbb{Q})$ and ϕ a morphism. We shall do this with the help of a 'height function' $h : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}$. We will see that if $\deg(\phi) \geq 2$, then $h(p) = 0$ if and only if p is preperiodic (theorem 4.4).

3 Height functions on $\mathbb{P}^n(\mathbb{Q})$

Let $n \geq 1$. We want to define a function $H : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}$ that measures the 'arithmetic complexity' of the points in $\mathbb{P}^n(\mathbb{Q})$. For example, for $n = 1$, we would like the point $(41 : 42)$ to have a higher complexity than $(1 : 1)$. Also, for a given $B \in \mathbb{R}_{>0}$, we want to have only finitely many points $p \in \mathbb{P}^n(\mathbb{Q})$ satisfying $H(p) \leq B$. These wishes lead to the following definition.

Definition 3.1. Let $p = (x_0 : x_1 : ... : x_n) \in \mathbb{P}^n(\mathbb{Q})$ be such that $x_0, x_1, ..., x_n$ are coprime integers. The *multiplicative height of* p is $H(p) = \max_i |x_i|$.

Note that for any $p = (x_0 : ... : x_n) \in \mathbb{P}^n(\mathbb{Q})$, we may assume $x_0, ..., x_n$ to be coprime integers. For if $x_i = \frac{a_i}{b_i}$, we may multiply by the lowest common multiple of $b_0, ..., b_n$ and then divide by any common factors. By the uniqueness (up to a factor -1) of such a representation of p, the height function is well defined. Note also that this definition fulfills our wish of only finitely many points $p = (x_0 : ... : x_n)$ satisfying $H(p) \leq B$ for a given $B \in \mathbb{R}_{>0}$: since it holds for every $i \in \{0, ..., n\}$ that $|x_i| \leq B$, every x_i can attain at most $2B + 1$ values, so there are at most $(2B + 1)^{n+1}$ possibilities for p.
Up to a scalar factor, morphisms of degree d turn out to raise the height of a point to the d-th power. The height function thus translates geometric information into arithmetic information.

Theorem 3.2. Let $\phi : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{P}^m(\mathbb{Q})$ be a morphism of degree d. There are constants $C_1, C_2 > 0$ such that for every $p \in \mathbb{P}^n(\mathbb{Q})$:

$$C_1 H(p)^d \leq H(\phi(p)) \leq C_2 H(p)^d.$$

For the computation of the lower bound scalar, we will use Hilbert's Nullstellensatz. This we quote and elucidate in appendix A.

Proof of theorem 3.2. Let us begin with a new notation. For a polynomial

$$f = \sum_{i_0,...,i_n} a_{i_0,...,i_n} X_0^{i_0} \cdots X_n^{i_n} \in \mathbb{C}[X_0, X_1, ..., X_n],$$

let $|f|$ denote the absolute value of the coefficient of f with the greatest absolute value: $|f| = \max_{i_0,...,i_n} |a_{i_0,...,i_n}|$.
The following observation will prove itself useful. If

$$F = \sum_{i_0,...,i_n} a_{i_0,...,i_n} X_0^{i_0} \cdots X_n^{i_n} \in \bar{\mathbb{Q}}[X_0, ..., X_n]$$

is homogeneous of degree d, then the number of terms of F is at most the number of monomials of degree d in $n+1$ variables, and this equals $\binom{n+d}{d}$. So if $p = (x_0, ..., x_n) \in \mathbb{P}^n(\mathbb{Q})$ is such that $x_0, ..., x_n \in \mathbb{Z}$ and $\gcd_i(x_i) = 1$, then by the triangle inequality we have:

$$\begin{aligned} |F(p)| = \left| \sum_{i_0,...,i_n} a_{i_0,...,i_n} x_0^{i_0} \cdots x_n^{i_n} \right| &\leq \sum_{i_0,...,i_n} |a_{i_0,...,i_n} x_0^{i_0} \cdots x_n^{i_n}| \\ &\leq \binom{n+d}{d} \cdot |F| \cdot (\max_i |x_i|)^d \\ &= \binom{n+d}{d} \cdot |F| \cdot H(p)^d. \end{aligned} \tag{5}$$

Now let ϕ be given by $\phi(p) = (F_0(p) : F_1(p) : ... : F_m(p))$. We note first that we may assume the coefficients of the F_j to be integers. For if not, we multiply every F_j by a common multiple c of all the denominators in their coefficients, giving polynomials $cF_j \in \mathbb{Z}[X_0, ..., X_n]$, for which it holds that $(cF_0(p) : ... : cF_m(p)) = (F_0(p) : ... : F_m(p))$ for all $p \in \mathbb{P}^n(\mathbb{Q})$.
Let $p = (x_0 : x_1 : ... : x_n) \in \mathbb{P}^n(\mathbb{Q})$ be such that $x_0, x_1, ..., x_n$ are coprime integers. For the computation of the upper bound scalar C_2, we observe that by (5):

$$H(\phi(p)) \leq \max_j |F_j(p)| \leq \binom{n+d}{d} \cdot \max_j |F_j| \cdot H(p)^d,$$

so it suffices to choose $C_2 = \binom{n+d}{d} \cdot \max_j |F_j|$.
Before we continue with the computation of the lower bound scalar C_1, we do some 'preparation work'. Since ϕ is a morphism, we know the F_j to have no common zeros in $\mathbb{P}^n(\bar{\mathbb{Q}})$, so by Hilbert's Nullstellensatz we may conclude:

$$\sqrt{(X_0, X_1, ..., X_n)} = \sqrt{(F_0, F_1, ..., F_m)} \subseteq \bar{\mathbb{Q}}[X_0, X_1, ...X_n].^2$$

In particular, $X_i \in \sqrt{(F_0, F_1, ..., F_m)}$ for every $i \in \{0, 1, ..., n\}$, i.e., $X_i^{a_i} \in (F_0, F_1, ..., F_m)$ for some integers a_i, thus

$$X_0^e, X_1^e, ..., X_n^e \in (F_0, F_1, ..., F_m)$$

for some common multiple e of the a_i. Hence there are polynomials $G_{ij} \in \bar{\mathbb{Q}}[X, Y]$ such that for every $i \in \{0, 1, ..., n\}$:

$$X_i^e = \sum_j G_{ij} F_j, \tag{6}$$

and these polynomials G_{ij} may be assumed to be homogeneous of degree $e - d$ and to have coefficients in $\mathbb{Q}$. Multiplying every G_{ij} by a common

[2]For the definition of $\sqrt{I}$, see appendix A.

multiple b of all the denominators in the coefficients of the G_{ij}, we find polynomials $H_{ij} = b \cdot G_{ij} \in \mathbb{Z}[X_0, ..., X_n]$ such that for every $i \in \{0, 1, ..., n\}$:

$$bX_i^e = \sum_j H_{ij} F_j. \tag{7}$$

Now let $p = (x_0 : ... : x_n) \in \mathbb{P}^n(\bar{\mathbb{Q}})$ be such that $x_0, ..., x_n \in \mathbb{Z}$ and $\gcd_i(x_i) = 1$. Evaluating (7) in p, we find for every x_i:

$$bx_i^e = \sum_j H_{ij}(p) F_j(p),$$

from which it follows that $\gcd_j(F_j(p))$ is a divisor of bx_i^e for every $i \in \{0, 1, .., n\}$. Since $\gcd_i(x_i^e) = 1$, it follows that $\gcd_j(F_j(p))$ is a divisor of b. Now because $\max_j(F_j(p)) = H(\phi(p)) \cdot \gcd_j(F_j)$, we find

$$\max_j(F_j(p)) \leq H(\phi(p)) \cdot b. \tag{8}$$

Let us now compute a lower bound scalar C_1. Evaluating (6) in p and applying (5) and (8), we find

$$\begin{aligned}
H(p)^e &= \max_i |x_i|^e \\
&= \max_i \left| \sum_{j=0}^{m} G_{ij}(p) F_j(p) \right| \\
&\leq \max_i \left\{ \binom{n+e-d}{e-d} H(p)^{e-d} \sum_{j=0}^{m} |G_{i,j}| \cdot |F_j(p)| \right\} \\
&\leq \binom{n+e-d}{e-d} H(p)^{e-d} (m+1) \cdot \max_{i,j} \{|G_{i,j}| \cdot |F_j(p)|\} \\
&\leq \binom{n+e-d}{e-d} H(p)^{e-d} (m+1) \cdot \max_{i,j} \{|G_{i,j}|\} \cdot b \cdot H(\phi(p)).
\end{aligned}$$

Dividing both sides by $H(p)^{e-d}$ gives

$$H(p)^d \leq \binom{n+e-d}{e-d} (m+1) \cdot \max_{i,j} \{|G_{i,j}|\} \cdot b \cdot H(\phi(p)),$$

whereupon we choose $C_1 = \left(\binom{n+e-d}{e-d} (m+1) \cdot \max_{i,j} \{|G_{i,j}|\} \cdot b \right)^{-1}$. □

Theorem 3.2 tells us that a morphism of degree d raises the height of a point approximately to the d-th power. This means that H is a multiplicative kind of function. Notationally, it is often more convenient to work with

an additive function.

Definition 3.4. The *logarithmic height* of a point $p \in \mathbb{P}^n(\mathbb{Q})$ is given by $h(p) = \log(H(p))$.

Notation 3.5. Let X be a set and let $f, g : X \to \mathbb{R}$. We write $f = g + O(1)$ if there is a constant C such that $|f(x) - g(x)| \leq C$ for every $x \in X$.

Using this notation, theorem 3.2 says that for a morphism ϕ of degree d: $h \circ \phi = dh + O(1)$.
Consider the morphism $\phi : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$ given by $\phi(x_0 : x_1) = (x_0^d : x_1^d)$. It is clear from the definition of the height function that

$$h(\phi(p)) = dh(p) \tag{9}$$

for all $p \in \mathbb{P}^1(\mathbb{Q})$. But theorem 3.2 gives us the less precise statement $h(\phi(p)) = dh(p) + O(1)$. We would like to define a new height function so that it gives us (9). For this we will use the following theorem.

Theorem 3.8. Let X be a set, $d > 1$ a real number and let $\phi : X \to X$ and $h : X \to \mathbb{R}$ be functions such that $h(\phi(x)) = dh((x)) + O(1)$ for all $x \in X$. The limit

$$\hat{h}(x) := \lim_{n \to \infty} \frac{1}{d^n} h(\phi^n(x))$$

exists for all $x \in X$. The function $\hat{h}$ satisfies:

(a) $\hat{h} = h + O(1)$

(b) $\hat{h} \circ \phi = d\hat{h}(x)$.

If $\hat{h}' : X \to \mathbb{R}$ is another function satisfying (a) and (b), then $\hat{h}' = \hat{h}$.

Proof. Let $x \in X$. To prove the existence of $\hat{h}(x)$, we will show that the sequence $(d^{-n} h(\phi^n(x)))_n$ is Cauchy. Now we are given a constant C such that $|h(\phi(y) - dh(y)| \leq C$ for all $y \in X$. For integers $n > m \geq 0$, we apply this with $y = \phi^{i-1}(x)$ to the telescoping sum:

$$\begin{aligned}
\left| \frac{1}{d^n} h(\phi^n(x)) - \frac{1}{d^m} h(\phi^m(x)) \right| &= \left| \sum_{i=m+1}^{n} \frac{1}{d^i} (h(\phi^i(x)) - dh(\phi^{i-1}(x)) \right| \\
&\leq \sum_{i=m+1}^{n} \frac{1}{d^i} |h(\phi^i(x)) - dh(\phi^{i-1}(x))| \\
&\leq \sum_{i=m+1}^{n} \frac{C}{d^i} \leq \sum_{i=m+1}^{\infty} \frac{C}{d^i} = \frac{C}{(d-1)d^m} \qquad (10)
\end{aligned}$$

From this we see that

$$\lim_{m,n\to\infty}\left|\frac{1}{d^n}h(\phi^n(x))-\frac{1}{d^m}h(\phi^m(x))\right|=0,$$

which shows that $(d^{-n}h(\phi^n(x)))_n$ is a Cauchy sequence. By the completeness of $\mathbb{R}$, we conclude that $\hat{h}(x)$ exists.
To prove (a), we consider (10) with $m=0$:

$$\left|\frac{1}{d^n}h(\phi^n(x))-h(x)\right|\leq\frac{C}{d-1}.$$

Letting n approach infinity, it follows that

$$|\hat{h}(x)-h(x)|\leq\frac{C}{d-1},$$

or $\hat{h}(x)=h(x)+O(1)$.
Property (b) is a direct consequence of the definition of $\hat{h}$:

$$\hat{h}(\phi(x))=\lim_{n\to\infty}\frac{1}{d^n}h(\phi^{n+1}(x))=d\cdot\lim_{n\to\infty}\frac{1}{d^{n+1}}h(\phi^{n+1}(x))=d\hat{h}(x).$$

Now let $\hat{h}':X\to\mathbb{R}$ be another function satisfying (a) and (b). We define $g=\hat{h}-\hat{h}'$ and observe: $g=O(1)$ and $g(\phi(x))=dg(x)$ for all $x\in X$. Thus for every positive integer n and every $x\in X$:

$$|d^ng(x)|=|g(\phi^n(x))|\leq C$$

for some constant C. Since we can take n arbitrary large, it follows that $g\equiv 0$, so $\hat{h}'=\hat{h}$. □

The following definition is now justified.

Definition 3.9. Let $\phi:\mathbb{P}^n(\mathbb{Q})\to\mathbb{P}^n(\mathbb{Q})$ be a morphism of degree $d\geq 2$. The *canonical height associated to* ϕ is the unique function $\hat{h}_\phi:\mathbb{P}^n(\mathbb{Q})\to\mathbb{R}$ satisfying $\hat{h}_\phi=h+O(1)$ and $\hat{h}_\phi(\phi(p))=d\hat{h}(p)$ for every $p\in\mathbb{P}^n(\mathbb{Q})$.

We have now developed enough terminology to state and prove some results relating heights to dynamics.

4 Arithmetic dynamics

Notation 4.1. In this section, H is as in definition 3.1, h is as in definition 3.4 and for ϕ a morphism, $\hat{h}_\phi$ is as in definition 3.9.

Theorem 4.2. Let $\phi:\mathbb{P}^n(\mathbb{Q})\to\mathbb{P}^n(\mathbb{Q})$ be a morphism of degree $d\geq 2$. There is a constant $B>0$ such that for every preperiodic point $p\in$

$\text{PrePer}(\phi) \subseteq \mathbb{P}^n(\mathbb{Q})$: $h(p) \leq B$.

Proof. By theorem 3.2, there is a constant $C > 0$ such that for any $r \in \mathbb{P}^n(\mathbb{Q})$:

$$h(\phi(r)) \geq dh(r) - C. \tag{11}$$

Applying this inequality to $\phi^{n-1}(r)$ yields $h(\phi^n(r)) \geq dh(\phi^{n-1}(r) - C)$. But to the right side of this inequality, we can apply (11) again, this time for $\phi^{n-2}(r)$. Continuing with this process, we find that

$$h(\phi^n(r)) \geq d^n h(r) - C(1 + d + d^2 + ... + d^{n-1}) \geq d^n(h(r) - C) \tag{12}$$

for every $r \in \mathbb{P}^n(\mathbb{Q})$. Now let $p \in \mathbb{P}^n(\mathbb{Q})$ be a preperiodic point, i.e., let $\phi^{m+n}(p) = \phi^m(p)$ for some $m \geq 0$ and $n \geq 1$. We can apply (12) with $r = \phi^m(p)$, from which we see

$$h(\phi^m(p)) = h(\phi^{m+n}(p)) = h(\phi^n(\phi^m(p)) \geq d^n(h(\phi^m(p)) - C),$$

and thus

$$h(\phi^m(p)) \leq \frac{d^n}{d^n - 1} C. \tag{13}$$

But since $d \geq 2$ and $n \geq 1$, we can bound the right side of (13) by $2C$, upon which we see that $h(\phi^m(p)) \leq 2C$. Combining this with (12) for $r = p$ and $n = m$ yields

$$h(p) \leq \frac{1}{d^m} h(\phi^m(p)) + C \leq \frac{1}{d^m} 2C + C \leq 3C,$$

so setting $B = 3C$ gives the desired result. □

Since we have seen there are only finitely many points of bounded height, the next result follows immediately.

Corollary 4.3. The set of preperiodic points $\text{PrePer}(\phi)$ of a morphism $\phi : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{P}^n(\mathbb{Q})$ of degree $d \geq 2$ is finite. □

Theorem 4.4. Let $\phi : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{P}^n(\mathbb{Q})$ be a morphism of degree $d \geq 2$. A point $p \in \mathbb{P}^n(\mathbb{Q})$ is preperiodic under ϕ if and only if $\hat{h}_\phi(p) = 0$.

Proof. Let $p \in \mathbb{P}^n(\mathbb{Q})$ be preperiodic. Then $\phi^n(p)$ attains only finitely many values, so

$$\hat{h}_\phi(p) = \lim_{n \to \infty} \frac{1}{d^n} h(\phi^n(p)) = 0.$$

Now let $p \in \mathbb{P}^n(\mathbb{Q})$ be such that $\hat{h}_\phi(p) = 0$. Then

$$h(\phi^n(p)) = \hat{h}_\phi(\phi^n(p)) + O(1) = d^n \hat{h}_\phi(p) + O(1) = O(1)$$

for all integers $n \geq 0$. There is thus a constant $B > 0$ such that $h(\phi^n(p)) \leq B$ for all integers $n \geq 0$, so $\phi^n(p)$ attains only finitely many points. We conclude that p is preperiodic. □

A The Zariski topology and Hilbert's Nullstellensatz

This appendix presents the Zariski Topology, to which we refer in our definition of rational maps, and Hilbert's Nullstellensatz, a classic result from algebraic geometry that we utilize in the proof of theorem 3.2.

Notation A.1. With K we will denote a number field. It's algebraic closure is $\bar{K}$.

Definition A.2. Let $I \subseteq \bar{K}[X_0, ..., X_n]$ be an ideal. The *radical of I* is the set

$$\sqrt{I} = \{f \in \bar{K}[X_0, ..., X_n] \mid f^n \in I \text{ for some } n \geq 0\},$$

where f^n denotes the nth power of f and not its nth iterate.

Definition A.3. An ideal $I \subseteq \bar{K}[X_0, ..., X_n]$ is called *homogeneous* if it is generated by homogeneous polynomials.

Definition A.4. Let $I \subseteq \bar{K}[X_0, ..., X_n]$ be a homogeneous ideal. The *algebraic set of I* is the set

$$V(I) = \{p \in \mathbb{P}^n(\bar{K}) \mid f(p) = 0 \text{ for all } f \in I\}.$$

Definition A.4: the Zariski topology. Let $\mathcal{I}$ denote the set of homogeneous ideals in $\bar{K}[X_0, ..., X_n]$. The *Zariski topology on* $\mathbb{P}^n(\mathbb{Q})$ is the set

$$\{U \subseteq \mathbb{P}^n(\mathbb{Q}) \mid \mathbb{P}^n(\mathbb{Q}) \backslash U = V(I) \text{ for some } I \in \mathcal{I}\}.$$

Theorem A.5: Hilbert's Nullstellensatz. Let $I, J \subsetneq \bar{K}[X_0, ..., X_n]$ be homogeneous ideals. Then $V(I) = V(J)$ if and only if $\sqrt{I} = \sqrt{J}$.

B Theorem 3.2 for $n = m = 1$

It turns out that for $n = m = 1$, theorem 3.2 can be proven without the use of Hilbert's Nullstellensatz. For convenience, we introduce one more definition before showing how it is done.

Definition B.1. A polynomial

$$f = \sum_{i_0,\dots,i_n} a_{i_0,\dots,i_n} X_0^{i_0} \cdots X_n^{i_n} \in \mathbb{Z}[X_1, ..., X_n]$$

is called *primitive* if $\gcd_{i_0,\dots,i_n}\{a_{i_0,\dots,i_n}\} = 1$.

Theorem B.2. Let $\phi : \mathbb{P}^1(\mathbb{Q}) \to \mathbb{P}^1(\mathbb{Q})$ be a morphism of degree d. There are constants $B_1, B_2 > 0$ such that for every $p \in \mathbb{P}^1(\mathbb{Q})$:

$$B_1 H(p)^d \leq H(\phi(P)) \leq B_2 H(p)^d.$$

Proof, not involving Hilbert's Nullstellensatz. Since we didn't use the Nullstellensatz for the computation of the upper bound scalar C_2 in the proof of theorem 3.2, our computation of B_2 comes down to setting $n = m = 1$ in that proof.
Let ϕ be given by $\phi(p) = (F_0(p) : F_1(p))$. We assume F_0 and F_1 to have coefficients in $\mathbb{Z}$ and to be primitive. For if the first is not the case, we multiply F_0 and F_1 by a common multitple of the denominators in the coefficients of F_0 and F_1, and if the second is not the case, we divide by any common factors these coefficients might have. Since for any $c \in \mathbb{Q}^*$ and any $p \in \mathbb{P}^1(\mathbb{Q})$ we have $(cF_0(p) : cF_1(p)) = (F_0(p) : F_1(p))$, our assumptions are justified.
Let $f_0 = F_0(X, 1)$ and $f_1 = F_1(X, 1) \in \mathbb{Q}[X]$. Suppose f_0 and f_1 have a common factor. As we saw in the proof of theorem 1.24, this would mean F_0 and F_1 have a common factor, contradicting definition 1.18. Thus f_0 and f_1 have no common factors. Also, from the fact that F_0 and F_1 are primitive, it follows directly that f_0 and f_1 are primitive. We conclude $\gcd(f_0, f_1) = 1$. Noting that $\mathbb{Q}[X]$ is a Euclidean domain, we apply the Euclidean algorithm to f_0 and f_1, finding polynomials $g_0, g_1 \in \mathbb{Q}[X]$ such that

$$g_0 f_0 + g_1 f_1 = 1. \tag{14}$$

Let $b = \deg(g_0) = \deg(g_1)$ and define $G_{10}, G_{11} \in \mathbb{Q}[X, Y]$ by $G_{10} = Y^b g_0(\frac{X}{Y})$ and $G_{11} = Y^b g_1(\frac{X}{Y})$. Since $F_0 = Y^d f_0(\frac{X}{Y})$ and $F_1 = Y^d f_1(\frac{X}{Y})$, it follows from (14) that

$$\begin{aligned} G_{10}F_0 + G_{11}F_1 &= Y^b g_0(\tfrac{X}{Y}) \cdot Y^d F_0(\tfrac{X}{Y}) + Y^b g_1(\tfrac{X}{Y}) \cdot Y^d F_1(\tfrac{X}{Y}) \\ &= Y^{b+d}\left(g_0(\tfrac{X}{Y}) f_0(\tfrac{X}{Y}) + g_1(\tfrac{X}{Y}) f_1(\tfrac{X}{Y})\right) \\ &= Y^{b+d}. \end{aligned}$$

In a similar way, we find polynomials G_0 and $G_1 \in \mathbb{Q}[X, Y]$ of equal degree a such that

$$G_0F_0 + G_1F_1 = X^{a+d}. \tag{15}$$

Without loss of generality we may assume $a \leq b$. Multiplying both sides of (15) by X^{b-a}, we find polynomials $G_{00} = X^{b-a}G_0$ and $G_{01} = X^{b-a}G_1$ such that

$$G_{00}F_0 + G_{01}F_1 = X^{b+d}.$$

For $i, j \in \{0, 1\}$, we multiply every G_{ij} by a common multiple c of all the denominators in their coefficients, obtaining polynomials $H_{ij} = cG_{ij} \in \mathbb{Z}[X, Y]$ such that

$$H_{00}F_0 + H_{01}F_1 = cX^{b+d} \qquad \text{and} \qquad H_{10}F_0 + H_{11}F_1 = cY^{b+d}. \tag{16}$$

Now let $p = (x : y) \in \mathbb{P}^1(\mathbb{Q})$ be such that x and y are coprime integers. Evaluating (16) in p gives

$$\begin{aligned} H_{00}(p)F_0(p) + H_{01}(p)F_1(p) &= cx^{b+d} \\ H_{10}(p)F_0(p) + H_{11}(p)F_1(p) &= cy^{b+d}, \end{aligned}$$

and it follows from this that $\gcd(F_0(p), F_1(p))$ is a divisor of both cx^{b+d} and cy^{b+d}. Since x^{b+d} and y^{b+d} are coprime, it must be that $\gcd(F_0(p), F_1(p))$ divides c. So by $\max(F_0(p), F_1(p)) = H(\phi(p)) \cdot \gcd(F_0(p), F_1(p))$, we conclude

$$\max(F_0(p), F_1(p)) \leq H(\phi(p)) \cdot c. \tag{17}$$

We now compute:

$$
\begin{aligned}
H(p)^{b+d} &= \max\{|x^{b+d}|, |y^{b+d}|\} \\
&= \max_{i\in\{0,1\}} |G_{i0}(p)F_0(p) + G_{i1}(p)F_1(p)| \\
&\leq 2 \cdot \max_{i,j\in\{0,1\}} |G_{ij}(p)F_j(p)| \\
&\leq 2 \cdot \max_{i,j\in\{0,1\}} \left|(b+1)\cdot|G_{ij}|\cdot H(p)^b \cdot F_j(p)\right| \\
&\leq 2(b+1)H(p)^b \cdot \max_{i,j\in\{0,1\}} \{|G_{ij}|\cdot H(\phi(p))\cdot c\} \\
&= 2c(b+1)H(p)^b \max_{i,j\in\{0,1\}} \{|G_{ij}|\}\cdot H(\phi(p)).
\end{aligned}
$$

Dividing both sides by $H(p)^b$ gives

$$H(p)^d \leq 2c(b+1) \max_{i,j\in\{0,1\}} \{|G_{ij}|\}\cdot H(\phi(p)),$$

and thus we choose

$$C_1 = 2c(b+1) \max_{i,j\in\{0,1\}} \{|G_{ij}|\}.$$

□

References

[1] Silverman, J.H. 2007. *The Arithmetic of Dynamical Systems*. Springer, New York.