Rational preperiodic points for rational maps

Jung Kyu CANCI
Supervisor: Prof. Pietro CORVAJA

a

a

a

a

a

Introduction

Let X be a set. Every map $\Phi\colon X \to X$ defines the *discrete dynamical system*

$$X \times \mathbb{Z} \to X \quad ; \quad X \times \mathbb{Z} \ni (x, n) \mapsto \Phi^n(x)$$

where Φ^n denotes the n-th iterate of Φ. We are interested to the case when $X = \mathbb{P}_1$ or $X = \mathbb{A}^1$ and Φ is the map given by a rational function $\phi \in \mathbb{C}(z)$ or a polynomial $\phi \in \mathbb{C}[z]$. Many arguments handled in the Theory of Dynamical Systems are useful in Number Theory and vice versa. Indeed there exists a wide literature which shows this connection. For example Furstenberg proved van der Waerden's Theorem on arithmetic progressions by using the Multiple Birkoff Recurrence Theorem (see [12]). In [33] Silverman shows some results about dynamical systems, similar to those treated in the present thesis, using some theorems of diophantine approximation, more precisely he used the finiteness of integral solutions to Thue's equations and Roth's Theorem.

The study of dynamical systems defined by polynomials or rational functions in the complex plane has a long history; for a large exposition see, e.g., [2][21].

In this thesis we study arithmetical problems about rational functions in one variable defined over a number field K. The main algebraic questions concern rational periodic (and more generally preperiodic) points for such functions, viewed as endomorphisms of the line. More precisely, we shall be interested in rational periodic points for functions having good reduction outside a prescribed set.

Before describing our original results, contained in Chapters 2 and 3, let us recall some known facts.

Let K a number field and let $\phi(z) \in K(z)$ be a rational function $\phi\colon K \to K$; ϕ defines a rational map $\Phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ defined over K. For all $P \in \mathbb{P}_1(K)$ the set

$$O_\Phi(P) = \{\Phi^i(P) \mid i \in \mathbb{N}\}$$

is called *forward orbit* or simply orbit of P under Φ. If $O_\Phi(P)$ is a finite set one says that P is a *preperiodic* point for Φ. In this situation it is clear that there exist two integers $n, m \in \mathbb{N}$ with $m \neq 0$ such that $\Phi^n(P) = \Phi^{n+m}(P)$. In this case one says that $\Phi^n(P)$ is a *periodic* point for Φ. If P is a periodic point for Φ then its orbit is called a *cycle* and if m is the smallest positive integer such that $\Phi^m(P) = P$ then m is called the *minimal* period of P for Φ. Moreover we say that m is the *length* of the cycle given by P and every element of this cycle is called a m-primitive periodic point for Φ.

Preperiodic points arise very naturally from the torsion in algebraic groups. Consider for instance the *multiplicative algebraic group* $\mathbb{G}_m$ (i.e. the affine variety $\mathbb{A}^1 \setminus 0$ endowed with the multiplicative group law.). In fact, for every positive integer n, the preperiodic points for the endomorphism z^n of $\mathbb{G}_m$ are the roots of unity. Another application concerns elliptic curves. In fact the torsion points of an elliptic curve E/K are exactly the preperiodic points of the multiplication-by-two map $P \mapsto 2P$. The quotient of E modulo multiplication by -1 is isomorphic with $\mathbb{P}_1$ and the multiplication-by-two map induces on the quotient a degree-4 map $\Phi\colon \mathbb{P}_1 \to \mathbb{P}_1$. Its preperiodic points correspond to the torsion points on E.

For a fixed endomorphism Φ of $\mathbb{P}_1$ defined over K of degree > 1, Northcott proved that Φ has only finitely many preperiodic points in $\mathbb{P}_1(K)$. (Actually Northcott's Theorem is much more general and also applies to certain endomorphisms of arbitrary varieties). By elementary height considerations it is easy to find an explicit bound for the cardinality of the set of all preperiodic points for Φ. In this way we obtain a rough estimation of the upper bound for the cycle lengths of Φ. On the other hand, by Lagrange's interpolation, it is easy to see that every n-tuple of distinct points of $\mathbb{P}_1(K)$ is a cycle for a suitable rational map (and even for a polynomial map). Therefore no uniform bound, depending only on K, is possible. Anyway, one can search for such uniform bounds holding for some particular infinite families of rational maps. In [22] Morton and Silverman considered the family of endomorphism of given degree. They conjectured that if $\Phi\colon \mathbb{P}_N \to \mathbb{P}_N$ is a morphism of degree $d \geq 2$ defined over K, then there exists a number k depending only on $[K : \mathbb{Q}]$, N and d such that the cardinality of the set of all K-rational preperiodic points for Φ is bounded by k. This conjecture is open even in the case of dimension 1. For instance no uniform bound is known for the minimal period of a rational periodic point for a quadratic map on $\mathbb{P}_1$.

Another natural infinite family of rational maps one can consider is the semigroup of endomorphism with good reduction outside a fixed finite set. Let us give a precise definition. Let K be a number field and let R be the ring of algebraic integers of K. We will say that a rational map $\Phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ defined over K has *good reduction* at a prime ideal $\mathfrak{p}$ of K if Φ can be written in the form $\Phi[X : Y] = [F(X, Y) : G(X, Y)]$, where F and G are homogeneous coprime polynomials of the same degree with coefficients in the local ring $R_{\mathfrak{p}}$ with the property that their resultant $\mathrm{Res}(F, G)$ is a $\mathfrak{p}$-unit.

In this thesis we will consider an arbitrary fixed finite set S of places of K containing all the archimedean ones. We will study arithmetical problems considering only the infinite family of rational maps from $\mathbb{P}_1$ to itself defined over K with good reduction outside S, i.e. the set of all the rational maps with good reduction at any prime ideal $\mathfrak{p} \notin S$. Such rational maps are characterized by the property of inducing an endomorphism (of the same degree) of $\mathbb{P}_1$ over the residue field corresponding to $\mathfrak{p}$, for all $\mathfrak{p} \notin S$. Note that every finitely generated semigroup of endomorphism of $\mathbb{P}_1$ is contained in such a semigroup.

In [22, Corollary B] Morton and Silverman proved a bound for the length of cycles in $\mathbb{P}_1(K)$ for endomorphism of $\mathbb{P}_1$ defined over K with degree ≥ 2 and good reduction outside S. This bound depends only on the cardinality of the set S. They used their results on multiplicity and reduction obtained in [23].

In this thesis we will show a new result about finite orbits. We will prove an effective bound for the cardinality of every finite orbit in $\mathbb{P}_1(K)$ (see Theorem 3.1 in Chapter 3), this extends the result by Morton and Silverman to cover also preperiodic points. Our bound depends only on the cardinality of the set S and on the class number of R_S. This result is reproduced in [7]. To prove this bound we shall use the Morton and Silverman's bound for cycle lengths and the S-unit equation Theorem in two and three variables. Hence our method depends on the (ineffective) Subspace Theorem.

For the polynomial case there existed a wide literature. In 1989 W. Narkiewicz in [24] proved the bound $C^{|S|^2+|S|[K:\mathbb{Q}]}$ for the length of every cycle in K for a monic polynomial in $R_S[z]$, where C is an absolute constant. Note that a monic polynomial in $R_S[z]$ defines a endomorphism of $\mathbb{A}^1$ defined over K with good reduction outside S. Narkiewicz used the the S-unit equation Theorem in two variables. In particular he applied the bound found by Evertse in [8].

Later T. Pezda was able to improve on Narkiewicz's bound. In [27] he studied cycle in R, a discrete valuation domain, for polynomial in $R[z]$. For the analogous problem in several variables see, e.g., [28]-[30][15].

Narkiewicz and Pezda in [25] proved a result that applied to the ring of S-integers R_S provides a bound for the cardinality of every finite orbit in R_S for a polynomial in $R_S[z]$. This bound depends only on the number of the prime ideals of bad reduction for the polynomial.

Recently R.L. Benedetto in [3] proved a statement similar to the Morton and Silverman's conjecture with $N = 1$. Indeed he has only considered the case where Φ is a endomorphism of $\mathbb{P}_1$ defined over K induced by a polynomial $\phi(z) \in K[z]$;

moreover his bound also depends on the number of prime ideals of bad reduction for Φ.

Another interesting question concerning rational maps with good reduction outside S is the following: considering the canonical equivalence for cycles given by the action of $\mathrm{PGL}_2(R_S)$ on $\mathbb{P}_1(K)$, *there exist only finitely many inequivalent cycles in $\mathbb{P}_1$ for rational maps with good reduction outside S ?* We solve this problem in chapter 2 of this thesis. We briefly introduce the statements of such results which are reproduced in [6]. Given a cycle $(P_0, P_1, \dots, P_{n-1})$ we consider the minimal ideal $\mathfrak{I}$ of R_S such that for every integer $0 \leq i \leq (n-1)$ $P_i \equiv P_{i+1} \pmod{\mathfrak{I}}$. Note that automatically all the points in the cycle will then be congruent modulo $\mathfrak{I}$. Given an ideal $\mathfrak{I}$ of R_S, we shall show in Theorem 2.1 that there exist only finitely many inequivalent cycles, for rational maps with good reduction outside S, where $\mathfrak{I}$ is the ideal satisfying the above property. An important tool used to prove this first main result of [6] is again the S-unit equation Theorem in two and three variables. Our second main result is Theorem 2.2, which states that if 2 is a S-unit then the ideal $\mathfrak{I}$ has infinitely many possibilities, even restricting to rational maps of degree equal to 4. It is easy to see that if two cycles are equivalent, then their associated ideals $\mathfrak{I}$ coincide. Hence Theorem 2.1 is in a sense best possible.

These last results are a sort of generalization of previous ones concerning only polynomials, viewed as endomorphism of $\mathbb{A}^1$, obtained in [13]. Using the S-unit equation Theorem in n variables with $n \in \{2, 3, 5\}$, Halter-Koch and Narkiewicz proved in particular that for any choice of S-integers $x, y \in R_S$, there exist only finitely many cycles, with given length, for polynomials in $R_S[z]$ which contain x, y as consecutive points. They also proved that there exist only finitely many possibilities for the non ordered couple (x, y), up to automorphisms of the line $\mathbb{A}^1$. This last result has no analogue in our situation, as already mentioned.

Our last result states that, fixed a cycle $(P_0, P_1, \dots, P_{n-1})$ in $\mathbb{P}_1(K)$ with $n \geq 4$, there exist only finitely many finite orbits, for rational maps with good reduction outside S, which contain the cycle $(P_0, P_1, \dots, P_{n-1})$.

0.1 The structure of this thesis

In **Chapter 1** we begin by giving a proof of the finiteness of periodic points of an endomorphism of $\mathbb{P}_1$. This proof is effective and is obtained, following Northcott, by using some elementary height considerations. The second section is dedicated to introduce the notion of good reduction for a map as given by Morton and Silverman in [23]. In the third section we define the good reduction for n-tuples in

$\mathbb{P}_1(K)$ at a prime ideal of K. Furthermore we show a finiteness result for n-tuples in $\mathbb{P}_1(K)$ with good reduction outside a fixed finite set of prime ideals of K, up to canonical equivalence. This is a direct application of Birch and Merriman's Theorem about the finiteness of classes of binary forms with given degree and discriminant. The content of this section is similar to the one with the same title "*Good reduction for n-tuples*"of [6]. We end this chapter by giving the proof of Morton and Silverman's bound for cycle lengths for rational map of degree ≥ 2 with good reduction outside S. By using an elementary argument we prove this bound also when the degree is 1.

In **Chapter 2** we present our finiteness results for cycles, which are reproduced in [6]. We start by proving some congruence properties of cycles for rational map. The method of proof is elementary and follows [23]. In the third section we present the proof of the already mentioned Theorem 2.1, which is the main theorem of Chapter 2. Furthermore we show a corollary which states that fixed two points $P_0, P_1 \in \mathbb{P}_1(K)$, there exist only finitely many cycles for rational maps, defined over K, with good reduction outside S, which contain as consecutive the points P_0 and P_1. We end this chapter by giving the proof of the already mentioned Theorem 2.2.

The first part of **Chapter 3** is dedicated to prove our bound which extends to preperiodic points the known results on periodic points. We end this chapter by showing some weak generalizations, to finite orbits, of the finiteness result about cycles presented in Chapter 2.

Contents

Chapter 1

Preliminaries

1.1 Finiteness of the preperiodic points of a rational map

Let K be a number field. This section is dedicated to prove a particular case of Northcott's theorem [26]. Indeed we will show the finiteness of preperiodic points in $\mathbb{P}_1(K)$ for a rational map on $\mathbb{P}_1$ defined over K with degree ≥ 2.

We denote by M_K the set of all places of K and by M_K^∞ the set of all the archimedean ones. For each $v \in M_K$ let $|\cdot|_v$ be the associated absolute value which extends one defined on $\mathbb{Q}$, namely: for $x \in \mathbb{Q}$ we have

$$|x|_v = \begin{cases} |x| & \text{if } v \text{ is archimedean} \\ |x|_p & \text{if } v \text{ is nonarchimedean} \end{cases}$$

where p is a prime number and $|p|_p = p^{-1}$. We denote by K_v the completion of the field K with respect the absolute value $|\cdot|_v$ and by $\mathbb{Q}_v$ the completion of $\mathbb{Q}$ with respect the absolute value $|\cdot|_p$, where $|\cdot|_v$ extends $|\cdot|_p$. The normalized absolute value $||\cdot||_v$ on K is defined by

$$||x||_v = |x|_v^{[K_v:\mathbb{Q}_v]/[K:\mathbb{Q}]} \text{ for all } x \in K,$$

so that the *product formula* holds:

$$\prod_{v \in M_K} ||x||_v = 1 \text{ for all } x \in K^*. \tag{1.1}$$

Given a point $P = [x_0 : \ldots : x_n] \in \mathbb{P}_n(K)$, we define its absolute multiplicative height

$$H(P) = \prod_{v \in M_K} \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}. \tag{1.2}$$

By the product formula, the product in (1.2) does not depend on the choice of homogeneous coordinates for P.

Now we show a fundamental result about the height $H(\cdot)$. Recall that the field of definition of a point $P = [x_0 : x_1 \ldots : x_n] \in \mathbb{P}_n(\bar{\mathbb{Q}})$ is the field

$$\mathbb{Q}(P) = \mathbb{Q}(x_0/x_i, x_1/x_i, \ldots, x_n/x_i) \text{ for any } i \text{ with } x_i \neq 0.$$

Theorem 1.1. *For any numbers $B, d \geq 0$, the set*

$$\left\{P \in \mathbb{P}_n(\bar{\mathbb{Q}}) \mid H(P) \leq B \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq d\right\}$$

is finite. In particular, for any fixed number field K, the set

$$\{P \in \mathbb{P}_n(K) \mid H(P) \leq B\}$$

is finite.

For a proof of this theorem see, for example, [17, Theorem B.2.3].

The following theorem is the key-step in the proof of Northcott's theorem. We present a proof which is practically the same proof of [17, Theorem B.2.5] in the particular case of one dimensional projective space. It provides a bound for the height of all preperiodic points for a given rational map.

Theorem 1.2. *Let K be a number field and let $\Phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ be a rational map of degree d defined over K. There exist two positive numbers $c_1 < 1$ and c_2 such that*

$$c_1 H(P)^d \leq H(\Phi(P)) \leq c_2 H(P)^d \tag{1.3}$$

holds for all $P \in \mathbb{P}_n(K)$. Furthermore c_1, c_2 are effectively computable in terms of Φ.

Proof. If $d = 0$ then the theorem is trivial. Suppose that $d \geq 1$. Write $\Phi([X : Y]) = [f_0(X,Y) : f_1(X,Y)]$ where f_0, f_1 are homogeneous polynomials in $K[X,Y]$ of same degree d with no common factors. For all indexes $i \in \{0,1\}$ we write f_i explicitly as

$$f_i(X,Y) = \sum_{0 \leq j \leq d} a_{i,j} X^{d-j} Y^j.$$

With (x, y) we shall always represent the homogeneous coordinates for a generic point of $P = [x : y] \in \mathbb{P}_1(K)$. For every absolute value $v \in M_K$ and for any point $P \in \mathbb{P}_1(K)$, we shall write $|P|_v = \max\{|x|_v, |y|_v\}$ (with abuse of notation, since $|P|_v$ depends on the given choice of coordinates). Moreover, for every positive number r we use the convenient notation

$$\epsilon_v(r) = \begin{cases} r & \text{if } v \text{ is archimedean} \\ 1 & \text{if } v \text{ is nonarchimedean.} \end{cases}$$

With this notation, the triangle inequality can be written uniformly as

$$|a_1 + a_2 + \ldots + a_r|_v \leq \epsilon_v(r) \max\{|a_1|_v, \ldots, |a_r|_v\}.$$

Therefore for every point $P \in \mathbb{P}_1(K)$, any $v \in M_K$ and all indexes $i \in \{0, 1\}$

$$\begin{aligned} |f_i(P)|_v &= \left|\textstyle\sum_{0\leq j\leq d} a_{i,j}x^{d-j}y^j\right|_v \\ &\leq \epsilon_v(d+1)\left(\max\nolimits_{0\leq j\leq d} |a_{i,j}|_v\right)\left(\max\nolimits_{0\leq j\leq d} |x^{d-j}y^j|_v\right) \quad \text{by triangle inequality} \\ &\leq \epsilon_v(d+1)\left(\max\nolimits_{0\leq j\leq d} |a_{i,j}|_v\right)(\max\{|x|_v, |y|_v\})^d \\ &= \epsilon_v(d+1)\left(\max\nolimits_{0\leq j\leq d} |a_{i,j}|_v\right)|P|_v^d. \end{aligned} \tag{1.4}$$

Now we have to use the identity

$$\prod_{v\in M_K} \epsilon_v(d+1)^{[K_v:\mathbb{Q}_v]/[K:\mathbb{Q}]} = \prod_{v\in M_K^\infty} \epsilon_v(d+1)^{[K_v:\mathbb{Q}_v]/[K:\mathbb{Q}]} = d+1.$$

Now take the maximum of (1.4) over $i \in \{0; 1\}$, raise to the $[K_v : \mathbb{Q}_v]/[K : \mathbb{Q}]$ power, and multiply over all $v \in M_K$. This gives

$$H(\Phi(P)) \leq c_2 H(P)^d$$

where

$$c_2 := (d+1) \prod_{v\in M_K} \max_{i\in\{0;1\}} \left\{ \max_{0\leq j\leq d} \left\|a_{i,j}\right\|_v \right\} > 0$$

so the second inequality in (1.3) holds.

Now, in order to obtain the constant c_1 of the first inequality in (1.3), we use the fact that f_0, f_1 are coprime polynomials. Indeed from this it follows that the resultant $\mathrm{Res}(f_0, f_1)$, of the polynomials f_0 e f_1, is non zero and that there exist four homogeneous polynomials $g_0, g_1, g_2, g_3 \in K[X, Y]$ with same degree $d - 1$ such that

$$f_0g_0 + f_1g_1 = \mathrm{Res}(f_0, f_1)X^{2d-1}; \quad f_0g_2 + f_1g_3 = \mathrm{Res}(f_0, f_1)Y^{2d-1}. \tag{1.5}$$

By easy computation, the polynomials $g_i's$ are effectively determinable, see for example [19].
For every index $0 \leq i \leq 3$ we explicitly write g_i as

$$g_i(X, Y) = \sum_{0 \leq j \leq d-1} b_{i,j} X^{d-1-j} Y^j.$$

Hence for all points $P \in \mathbb{P}_1$ and every valuation v it results that

$$\begin{aligned} |P|_v^{2d-1} &= \max\{|x|_v^{2d-1}, |y|_v^{2d-1}\} \\ &= |\mathrm{Res}(f_0, f_1)|_v^{-1} \max\{|(f_0 g_0 + f_1 g_1)(P)|_v, |(f_0 g_2 + f_1 g_3)(P)|_v\} \\ &\leq |\mathrm{Res}(f_0, f_1)|_v^{-1} \epsilon_v(2) \left(\max_{0 \leq i \leq 3} |g_i(P)|_v\right) \left(\max_{0 \leq i \leq 1} |f_i(P)|_v\right) \\ &\leq |\mathrm{Res}(f_0, f_1)|_v^{-1} \epsilon_v(2) \left[\epsilon_v(d) \left(\max_{i,j} |b_{i,j}|_v\right) |P|_v^{d-1}\right] \left(\max_i |f_i(P)|_v\right). \end{aligned}$$

Now raising to the $[K_v : \mathbb{Q}_v]/[K : \mathbb{Q}]$ power, and taking the product over all $v \in M_K$, by the product formula applied to $\mathrm{Res}(f_0, f_1)^{-1}$ we obtain that

$$c_1 H(P)^{2d-1} \leq H(P)^{d-1} H(\Phi(P))$$

where

$$c_1 := \left[2d \prod_{v \in M_K} \max_{i,j} \left\|b_{i,j}\right\|_v\right]^{-1} > 0.$$

Note that $\left(\prod_{v \in M_K} \max_{i,j} \left\|b_{i,j}\right\|_v\right)$ is the multiplicative height of a point of $\mathbb{P}_{4d-1}(K)$. By definition, $H(\cdot)$ always assumes values ≥ 1. From this it is clear that $c_1 < 1$. □

Theorem 1.3. *Let $\Phi \colon \mathbb{P}_1 \to \mathbb{P}_1$ be a rational map of degree $d \geq 2$ defined over a number field K. Then there exist only finitely many preperiodic points for Φ.*

Proof. By Theorem 1.2 there exist a positive constant $c_1 < 1$ such that

$$H(\Phi(P)) \geq c_1 H(P)^d \quad \text{holds for every point } P \in \mathbb{P}_1(K). \tag{1.6}$$

If $P \in \mathbb{P}_1(K)$ is a preperiodic point for Φ, then the sequence $\{H(\Phi^n(P))\}_{n \in \mathbb{N}}$ is bounded. Instead, from (1.6) and $d \geq 2$, if P is such that $c_1 H(P)^d > H(P)$, then $\{H(\Phi^n(P))\}_{n \in \mathbb{N}}$ is an unbounded sequence. Therefore, if P is a preperiodic point, then $H(P) \leq c_1^{\frac{1}{1-d}}$. Note that $c_1^{\frac{1}{1-d}} > 1$. We conclude the proof by applying Theorem 1.1. □

1.2 Good reduction for rational maps

In this thesis we shall use the following notation:

K a number field;

R the ring of integers of K;

$\mathfrak{p}$ a non zero prime ideal of R;

$R_{\mathfrak{p}}$ the local ring of R at the prime ideal $\mathfrak{p}$;

$m_{\mathfrak{p}}$ the maximal ideal of $R_{\mathfrak{p}}$ (which is principal);

$K(\mathfrak{p})$ $=R/\mathfrak{p} \cong R_{\mathfrak{p}}/m_{\mathfrak{p}}$ the residue field of the prime ideal $\mathfrak{p}$;

$v_{\mathfrak{p}}$ the $\mathfrak{p}$-adic valuation on R corresponding to the prime ideal $\mathfrak{p}$ (we always assume $v_{\mathfrak{p}}$ to be normalized so that $v_{\mathfrak{p}}(K^*) = \mathbb{Z}$);

S a fixed finite set of places of K of cardinality s including all the archimedean ones.

We denote the ring of S-integers by

$$R_S := \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0 \text{ for every prime ideal } \mathfrak{p} \notin S\}$$

and the group of S-units by

$$R_S^* := \{x \in K^* \mid v_{\mathfrak{p}}(x) = 0 \text{ for every prime ideal } \mathfrak{p} \notin S\}.$$

To give the next definition we need the canonical (mod $\mathfrak{p}$)-projection from $\mathbb{P}_1(K)$ to $\mathbb{P}_1(K(\mathfrak{p}))$. It is defined in the following way: since $m_{\mathfrak{p}}$ is a principal ideal, every point $P \in \mathbb{P}_1(K)$ can be represented by homogeneous coordinates $P = [x : y]$ such that $x, y \in R_{\mathfrak{p}}$ and they do not belong simultaneously to $m_{\mathfrak{p}}$, so that the point $[x + m_{\mathfrak{p}} : y + m_{\mathfrak{p}}] \in \mathbb{P}_1(R_{\mathfrak{p}}/m_{\mathfrak{p}})$ is well defined. By the canonical isomorphism $R_{\mathfrak{p}}/m_{\mathfrak{p}} \cong K(\mathfrak{p})$, for every point $P \in \mathbb{P}_1(K)$ it is possible to associate a point of $\mathbb{P}_1(K(\mathfrak{p}))$ which will be called the *reduction modulo* $\mathfrak{p}$ of P. We use the same definition of good reduction, at a prime ideal, for a rational map used in [23] or [6].

Definition 1.1. *We say that a morphism* $\Phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ *defined over K has good reduction at a prime ideal* $\mathfrak{p}$ *if there exists a morphism* $\tilde{\Phi}\colon \mathbb{P}_1 \to \mathbb{P}_1$ *defined over* $K(\mathfrak{p})$ *with* $\deg \Phi = \deg \tilde{\Phi}$ *such that the following diagram*

$$\begin{tikzcd}
\mathbb{P}_{1,K} \arrow[r, "\Phi"] \arrow[d, "\sim"'] & \mathbb{P}_{1,K} \arrow[d, "\sim"] \\
\mathbb{P}_{1,K(\mathfrak{p})} \arrow[r, "\widetilde{\Phi}"] & \mathbb{P}_{1,K(\mathfrak{p})}
\end{tikzcd}$$

is commutative, where ˜ denotes the reduction modulo $\mathfrak{p}$. Furthermore if Φ has good reduction at every prime ideal $\mathfrak{p} \notin S$, we say that it has good reduction outside S.

We shall consider only cycles for rational maps with good reduction outside S. By definition it is clear that these maps form a semigroup under composition on which the group $\mathrm{PGL}_2(R_S)$ acts by conjugation.

Now we give an equivalent version of the previous definition which is useful to determine when a rational map has good reduction at a prime ideal $\mathfrak{p}$.

Let $\Phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ a rational map defined over K by $\Phi([X : Y]) = [F(X,Y) : G(X,Y)]$ where F, G are homogeneous polynomials in $R[X,Y]$ with the same degree d and no common factors. Since $R_\mathfrak{p}$ is a P.I.D. we may assume that F, G have coefficients in $R_\mathfrak{p}$ and that at least one coefficient is in $R_\mathfrak{p}^*$. Therefore, by reduction modulo $\mathfrak{p}$ of the coefficients of F and G, we obtain two homogeneous polynomials $\tilde{F}, \tilde{G} \in K(\mathfrak{p})[X,Y]$ which are not both the zero polynomial. In this way it is well defined the rational map

$$\tilde{\Phi}\colon \mathbb{P}_1 \to \mathbb{P}_1;\ \ \tilde{\Phi}([x : y]) = [\tilde{F}(x,y) : \tilde{G}(x,y)], \tag{1.7}$$

defined over $K(\mathfrak{p})$. Now it is easy to see that the rational map Φ has good reduction at a prime ideal $\mathfrak{p}$ if and only if $\tilde{F}(x,y)$ and $\tilde{G}(x,y)$ are coprime homogeneous polynomials in $K(\mathfrak{p})[X,Y]$. Therefore the rational map Φ has good reduction at the prime ideal $\mathfrak{p}$ if and only if $\mathrm{Res}(\tilde{F},\tilde{G})$ is non zero in $K(\mathfrak{p})$; or equivalently if and only if $\mathrm{Res}(F,G) \notin m_\mathfrak{p}$. In this case the regular map defined in (1.7) is the rational map which appears in the Definition 1.1.

Morton and Silverman gave also another method to see when the rational map Φ has good reduction at a prime ideal $\mathfrak{p}$. They introduced the definition of discriminant of a rational map in the following way: to ease notation, if $H(t_1,\dots,t_k) \in K[t_1,\dots,t_k]$ is a non zero polynomial we define $v_\mathfrak{p}(H)$ as

$$v_\mathfrak{p}(H) = v_\mathfrak{p}\left(\sum_I a_I t_1^{i_1} \cdots t_k^{i_k}\right) = \min_I v_\mathfrak{p}(a_I) \tag{1.8}$$

where the minimum is taken over all multi-indexes $I = (i_i, \dots, i_k)$. That is, $v_{\mathfrak{p}}(H)$ is the smallest valuation of the coefficients of H. For any family of polynomials $H_1, \dots, H_m \in K[t_1, \dots, t_k]$ we define $v_{\mathfrak{p}}(H_1, \dots, H_m)$ to be the minimum of the $v_{\mathfrak{p}}(H_i)$ with $i \in \{1, \dots, m\}$. The discriminant $\mathrm{Disc}(\Phi)$ of the rational map Φ is the ideal of R whose valuation at a prime ideal $\mathfrak{p}$ is given by

$$v_{\mathfrak{p}}(\mathrm{Disc}(\Phi)) = v_{\mathfrak{p}}(\mathrm{Res}(F, G)) - 2d v_{\mathfrak{p}}(F, G).$$

By the properties of the resultant this definition is a good one; i.e. it is independent on the choice of the homogeneous coefficients of the polynomials F and G.
For every prime ideal $\mathfrak{p}$ it is easy to see that Φ has good reduction at $\mathfrak{p}$ if and only if $v_{\mathfrak{p}}(\mathrm{Disc}(\Phi)) = 0$. In this way, for every prime ideal $\mathfrak{p}$, we have a simple condition to prove when the rational map Φ has good reduction at $\mathfrak{p}$.

1.3 Good reduction for n-tuples

Let, as before, S be a finite set of places of K, containing all the archimedean ones. This section is dedicated to explain the notion of good reduction at a prime ideal for a n-tuple. Some arguments contained in this section are strictly related to the cycles for rational maps with good reduction outside S. Indeed some methods used in the proofs contained in this section will be useful in the next chapters.
We begin by giving a proposition that is useful when R_S is not a P.I.D..

Proposition 1.1. *There exist a finite set S_R of places of K and an integral number C such that every point $P \in \mathbb{P}_1(K)$ can be represented by S-integral homogeneous coordinates (x, y) which satisfy* $\min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\} = 0$ *for all prime ideals $\mathfrak{p} \notin S_R$ and* $\min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\} \leq C$ *for every $\mathfrak{p} \in S_R$.*

Proof. Since the ring R_S is a Dedekind domain, every ideal of R_S can be generated by two elements. Let us denote by h_S the class number of R_S. Let

$$R_S, (a_2R_S + b_2R_S), \dots, (a_{h_S}R_S + b_{h_S}R_S)$$

be a set of representatives for the ideal classes.

Each point $P \in \mathbb{P}_1(K)$ can be expressed by integral coordinates $P = [\bar{x} : \bar{y}]$. The ideal $(\bar{x}R_S + \bar{y}R_S)$ is equivalent to one of the just chosen representatives. Hence there exist two integers c and d in R_S such that

$$c(\bar{x}R_S + \bar{y}R_S) = dR_S$$

or

$$c(\bar{x}R_S + \bar{y}R_S) = d(a_iR_S + b_iR_S)$$

for a suitable index $i \in \{2, \dots, h_S\}$. Let $x = c\bar{x}/d$ and $y = c\bar{y}/d$; note that x, y are integers. In the first case one has that $(xR_S + yR_S) = R_S$, thus

$$\min\{v_\mathfrak{p}(x), v_\mathfrak{p}(y)\} = 0$$

for every prime ideal $\mathfrak{p} \notin S$. Otherwise one has that $(xR_S + yR_S) = (a_iR_S + b_iR_S)$, thus

$$\min\{v_\mathfrak{p}(x), v_\mathfrak{p}(y)\} = \min\{v_\mathfrak{p}(a_i), v_\mathfrak{p}(b_i)\}$$

for every prime ideal $\mathfrak{p} \notin S$.

Now it is sufficient to choose S_R as the set of nonarchimedean places of K such that $\min\{v_\mathfrak{p}(a_i), v_\mathfrak{p}(b_i)\} \neq 0$ for some indexes $i \in \{2, \dots, h_S\}$ and

$$C = \max_{\mathfrak{p} \in S_R} \left\{ \min\{v_\mathfrak{p}(a_i), v_\mathfrak{p}(b_i)\} \mid i \in \{2, \dots, h_S\} \right\}.$$

□

Remark 1.1. By [20, Corollary 2 to Theorem 36, Chapter 5] it follows that we can choose every representative $(a_iR_S + b_iR_S)$ such that its norm is bounded by a constant λ depending only on K. Thus

$$\|(a_iR_S + b_iR_S)\| = \prod_{\mathfrak{p} \in S_R \setminus S} \|\mathfrak{p}\|^{\min\{v_\mathfrak{p}(a_i), v_\mathfrak{p}(b_i)\}} \leq \lambda$$

for all $i \in \{2, \dots, h_S\}$. From this we deduce that $\|\mathfrak{p}\| \leq \lambda$ for every $\mathfrak{p} \in S_R \setminus S$ and we can choose

$$\min\{v_\mathfrak{p}(a_i), v_\mathfrak{p}(b_i)\} \leq C \leq \log_2 \lambda. \tag{1.9}$$

By [20, Corollary 2 to Theorem 37, Chapter 5]

$$\lambda \leq \frac{[K : \mathbb{Q}]!}{[K : \mathbb{Q}]^{[K:\mathbb{Q}]}} \left(\frac{4}{\pi}\right)^c |\mathrm{disc}(R)|^{\frac{1}{2}}$$

where c denote the cardinality of the set of all not real embeddings of K in $\mathbb{C}$.

Proposition 1.1 allows to adopt the following convention: writing $P = [x : y]$ for a generic element of $\mathbb{P}_1(K)$ we shall always choose $x, y \in R_S$ with the property just described and we shall say that x and y are *almost coprime* S-integers.

Notation. In the present section every point will be represented by almost coprime coordinates, except in the cases in which it will be explicitly specified. Moreover for any n-tuple $(P_0, P_1, \dots, P_{n-1})$ of points of $\mathbb{P}_1(K)$, for every index i, the vector (x_i, y_i) will always represent almost coprime integral homogeneous coordinates for the point P_i.

Definition 1.2. *Let $\mathfrak{p}$ be a prime ideal of K. We say that a n-tuple $(P_0, \dots, P_{n-1})$ of elements of $\mathbb{P}_1(K)$ has good reduction at $\mathfrak{p}$ if the n-tuple formed by the reduction modulo $\mathfrak{p}$ has n distinct elements in $\mathbb{P}_1(K(\mathfrak{p}))$; a n-tuple has good reduction outside S if it has good reduction at every prime ideal $\mathfrak{p} \notin S$.*

Now we introduce a “distance”, already used by Morton and Silverman in [23], which characterizes the n-tuples of good reduction at a prime ideal $\mathfrak{p}$.

Let $P_1 = [x_1 : y_1], P_2 = [x_2 : y_2] \in \mathbb{P}_1(K)$ and $\mathfrak{p}$ be a prime ideal of R. We denote by

$$\delta_{\mathfrak{p}}(P_1, P_2) = v_{\mathfrak{p}}(x_1y_2 - x_2y_1) - \min\{v_{\mathfrak{p}}(x_1), v_{\mathfrak{p}}(y_1)\} - \min\{v_{\mathfrak{p}}(x_2), v_{\mathfrak{p}}(y_2)\} \quad (1.10)$$

the $\mathfrak{p}$-adic logarithmic distance; $\delta_{\mathfrak{p}}(P_1, P_2)$ is independent of the choice of the homogeneous coordinates, i.e. it is well defined, takes integral values and the following properties hold:

$$\begin{array}{lll} \delta_{\mathfrak{p}}(P, Q) \geq 0 & \text{for every } P \text{ and } Q & (\delta') \\ \delta_{\mathfrak{p}}(P, Q) \geq 1 & \text{if and only if } P \equiv Q \pmod{\mathfrak{p}} & (\delta'') \\ \delta_{\mathfrak{p}}(P, Q) = \infty & \text{if and only if } P = Q & (\delta''') \end{array} \quad (1.11)$$

By property (δ'') it follows that a n-tuple $(P_0, P_1, \dots, P_{n-1}) \in \mathbb{P}_1^n(K)$ has good reduction outside S if and only if $\delta_{\mathfrak{p}}(P_i, P_j) = 0$ for every prime ideal $\mathfrak{p} \notin S$ and for all distinct indexes $i, j \in \{0, \dots, n-1\}$.

Now we use the canonical action of the automorphism-group $\mathrm{PGL}_2(R_S)$ on $\mathbb{P}_1(K)$ to give the following:

Definition 1.3. *Two n-tuples $(P_0, \dots, P_{n-1})$ and $(Q_0, \dots, Q_{n-1})$ are called equivalent if there exists a projective automorphism $A \in \mathrm{PGL}_2(R_S)$ such that*

$$A(P_i) = Q_i \textit{ for all } i \in \{0, 1, \dots, n-1\}.$$

It is clear that a n-tuple $(P_0, P_1, \dots, P_{n-1})$ has good reduction outside S if and only if every n-tuple equivalent to $(P_0, P_1, \dots, P_{n-1})$ has good reduction outside S.

If R_S is a P.I.D., then for any point of $\mathbb{P}_1(K)$ we can choose coprime integral homogeneous coordinates. In this way, for any n-tuple $(P_0, P_1, \ldots, P_{n-1})$ with good reduction outside S and for every prime ideal $\mathfrak{p} \notin S$, it follows that

$$v_{\mathfrak{p}}(x_i y_j - x_j y_i) = \delta_{\mathfrak{p}}(P_i, P_j) = 0,$$

therefore $x_i y_j - x_j y_i$ is a S-unit.
But in any case the useful following lemma holds.

Lemma 1.1. *There exists a finite set $\mathcal{R} \subset R_S$ which satisfies the following property: for every n-tuple $(P_0, P_1, \ldots, P_{n-1})$ of good reduction outside S and for every couple of distinct indexes $i, j \in \{0, \ldots, n-1\}$ there exist an integer $r_{i,j} \in \mathcal{R}$ and a unit $u_{i,j} \in R_S^*$ such that*

$$x_i y_j - x_j y_i = r_{i,j} u_{i,j}.$$

Proof. Let $(P_0, P_1, \ldots, P_{n-1})$ be a n-tuple of good reduction outside S. For every $\mathfrak{p} \notin S$ and every couple of distinct indexes $0 \le i, j \le (n-1)$, by definition of logarithmic distance we have that

$$v_{\mathfrak{p}}(x_i y_j - x_j y_i) = \min\{v_{\mathfrak{p}}(x_i), v_{\mathfrak{p}}(y_i)\} + \min\{v_{\mathfrak{p}}(x_j), v_{\mathfrak{p}}(y_j)\}.$$

Let C and S_R be the integer and the set defined in the Proposition 1.1. Having chosen almost coprime homogeneous coordinates, for every $\mathfrak{p} \in S_R/S$, it follows that $v_{\mathfrak{p}}(x_i y_j - x_j y_i) \le 2C$, and for every other prime ideal not in S it follows that $v_{\mathfrak{p}}(x_i y_j - x_j y_i) = 0$. Therefore for every couple of distinct points $P_i = [x_i : y_i], P_j = [x_j : y_j]$ included in the n-tuple $(P_0, P_1, \ldots, P_{n-1})$ the following principal ideal of R_S

$$(x_i y_j - x_j y_i) R_S = \prod_{\mathfrak{p} \in S_R \setminus S} \mathfrak{p}^{v_{\mathfrak{p}}(x_i y_j - x_j y_i)}$$

is an element of the finite set

$$\left\{ \prod_{\mathfrak{p} \in S_R \setminus S} \mathfrak{p}^{e_{\mathfrak{p}}} \mid 0 \le e_{\mathfrak{p}} \le 2C \right\}. \tag{1.12}$$

Now is clear that the proof follows by choosing $\mathcal{R}$ the finite set composed by taking a generator for each principal ideal contained in (1.12). Note that this set has cardinality bounded by $(2C+1)^{|S_R \setminus S|}$. □

Proposition 1.2. *The set of equivalence classes of n-tuples in $\mathbb{P}_1(K)$ with good reduction outside S is finite.*

In the following proof we shall consider some binary forms. Two binary forms $G(X,Y)$ and $H(X,Y)$ are called equivalent if there exists a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(R_S)$$

such that $G(X,Y) = H(aX+bY, cX+dY)$. We shall use the Birch and Merriman's Theorem [5] about the finiteness of classes of binary forms with given degree and discriminant.

Proof of Proposition 1.2. Note that for a large n there are not n-tuples with good reduction outside S. Indeed, let $m = \min_{\mathfrak{p}\notin S}\{|K(\mathfrak{p})|\}$. For every prime ideal $\mathfrak{p}$ which realizes the minimum m we have that $|\mathbb{P}_1(K(\mathfrak{p}))| = m+1$. From this it follows that there can exist n-tuple of good reduction outside S only if $n \leq m+1$.

For $n = 1$ the number of equivalence classes is the order h_S of the ideal class group of R_S. We choose representatives for every class and express them, except the trivial ideal R_S, through two generators $(a_2R_S + b_2R_S), \ldots, (a_{h_S}R_S + b_{h_S}R_S)$. Note that these representatives define h_S points $[0:1], [a_2:b_2], \ldots, [a_{h_S}:b_{h_S}]$ of $\mathbb{P}_1(K)$ pairwise inequivalent for the action of $\mathrm{PGL}_2(R_S)$. Now we prove that every point $P \in \mathbb{P}_1(K)$ belongs to the orbit of [1:0] or of a point $[a_i:b_i]$ with $i \in \{2,\ldots,h_S\}$.

Let $P \in \mathbb{P}_1(K)$. We write it with integral coordinates $P = [\bar{x}:\bar{y}]$. If $(\bar{x}R_S + \bar{y}R_S)$ is a principal ideal, then P is an element of the orbit of $[1:0]$ under the action of $\mathrm{PGL}_2(R_S)$. Indeed, let $(\bar{x}R_S + \bar{y}R_S) = aR_S$ for a suitable $a \in R_S$. It is clear that $x = \bar{x}/a$ and $y = \bar{y}/a$ are elements of R_S such that $(xR_S + yR_S) = R_S$. This is equivalent to the existence of two S-integers r_x and r_y such that $xr_x + yr_y = 1$. Therefore the matrix

$$\begin{pmatrix} r_x & r_y \\ -y & x \end{pmatrix} \in \mathrm{SL}_2(R_S)$$

and maps the point $[x:y]$ to $[1:0]$.

Otherwise, there exist $c,d \in R_S$ such that $c(\bar{x}R_S + \bar{y}R_S) = d(a_iR_S + b_iR_S)$ for one index $i \in \{2,\ldots,h_S\}$. Therefore, the S-integers $x = c\bar{x}/d$ and $y = c\bar{y}/d$ generate the ideal

$$(xR_S + yR_S) = (a_iR_S + b_iR_S) = I \subset R_S.$$

By definition of I^{-1}, there are elements $x', y' \in I^{-1}$ satisfying $xy' - yx' = 1$, namely

$$\begin{pmatrix} x & x' \\ y & y' \end{pmatrix} \in \mathrm{SL}_2(K).$$

Moreover there are $a'_i, b'_i \in I^{-1}$ such that $a_i b'_i - b_i a'_i = 1$, namely

$$\begin{pmatrix} a_i & a'_i \\ b_i & b'_i \end{pmatrix} \in \mathrm{SL}_2(K).$$

So that the following matrix

$$\begin{pmatrix} a_i & a'_i \\ b_i & b'_i \end{pmatrix} \begin{pmatrix} x & x' \\ y & y' \end{pmatrix}^{-1} = \begin{pmatrix} a_i & a'_i \\ b_i & b'_i \end{pmatrix} \begin{pmatrix} y' & -x' \\ -y & x \end{pmatrix} = \begin{pmatrix} a_i y' - y a'_i & -a_i x' + x a'_i \\ y' b_i - y b'_i & -x' b_i + x b'_i \end{pmatrix} \in \mathrm{SL}_2(R_S)$$

maps $[x : y]$ to $[a_i : b_i]$. This concludes the case $n = 1$.

Let $n \geq 2$ and $(P_0, P_1, \dots, P_{n-1})$ be a n-tuple with good reduction outside S. By Lemma 1.1 we obtain for every distinct indexes i, j the following identity

$$x_i y_j - x_j y_i = r_{i,j} u_{i,j}, \tag{1.13}$$

where $u_{i,j} \in R_S^*$ and $r_{i,j} \in \mathcal{R}$.

For all distinct indexes $0 \leq i, j \leq (n-1)$ we fix a possible values of $r_{i,j} \in \mathcal{R}$. For each n-tuple $(P_0, P_1, \dots, P_{n-1})$, which verifies the identities (1.13), we associate the following binary form of degree n

$$F(X, Y) = \prod_{0 \leq i \leq n-1} (x_i X - y_i Y),$$

defining in this way a family of forms with discriminant

$$D(F) = u \left(\prod_{0 \leq i < j \leq n-1} r_{i,j}^2 \right), \tag{1.14}$$

where u is a variable S-unit.

Dirichlet unit Theorem states that the group of S-units R_S^* is a finitely generated group of rank equal to $|S| - 1$. From this theorem it is easy to see that there exists a finite set $\mathcal{V} \subset R_S^*$, of cardinality $(2n-3)^{|S|-1}$, such that every S-unit is representable as product of a $(2n-2)$-power of an S-unit and an element of $\mathcal{V}$. Therefore, for every n-tuple $(P_0, P_1, \dots, P_{n-1})$ which satisfies the identities (1.13), the unit u which appears in the equation (1.14) can be written as $u = v\lambda^{2n-2}$ with $v \in \mathcal{V}$ and $\lambda \in R_S^*$. Thus, if we replace the coordinates (x_0, y_0) of P_0 with $(x_0\lambda^{-1}, y_0\lambda^{-1})$, then we obtain a new binary form with discriminant $v \prod r_{i,j}^2$.
In other words, with an appropriate choice of coordinates, the n-tuples which satisfy the identities (1.13), with fixed $r_{i,j}$, define a family of binary forms of degree

n with discriminant $v \prod r_{i,j}^2$ for a suitable $v \in \mathcal{V}$. The equivalence of binary forms associated with n–tuples coincides with the equivalence of the corresponding unordered n–tuples. By Birch and Merriman' Theorem contained in [5] we know that the number of classes of binary forms of degree n with fixed discriminant $v \prod r_{i,j}^2$ is finite. Now the proof follows from the finiteness of the sets $\mathcal{V}$ and $\mathcal{R}$. □

If $K = \mathbb{Q}$, then it is clear that $\mathcal{R} = \{1\}$. Moreover it is easy to determine the set $\mathcal{V}$ for every given set S. Therefore, in this case, the previous proof becomes effective by using the Evertse and Győry's result obtained in [10].

1.4 A bound for cycle lengths for rational maps

This section is dedicated to prove the Morton and Silverman's bound for cycle lengths for rational maps with good reduction outside S. The proofs contained in this section are the same ones contained in [22], [23].

Morton and Silverman in [23] describe a general theory of multiplicity for periodic points on smooth projective varieties, obtaining some significant results that they use in [22] to obtain the bound that we shall use in the next chapters.

Let X/K be a smooth projective variety, actually in this thesis we are interested to case when $X = \mathbb{P}_1$, and Φ is an endomorphism of X defined over K. Morton and Silverman use intersection theory to assign a multiplicity to each periodic point. We recall that a point $P \in X$ is a n-periodic point for a rational map Φ if $\Phi^n(P) = P$ and we say that P is a primitive n-periodic point if n is the minimal period of P.

Let

$$\Delta(X) \subset X \times X$$

be the diagonal and let

$$\Gamma(\Phi) = \{(x, \Phi(x)) \mid x \in X\} \subset X \times X$$

be the graph of Φ. We say that a map Ψ is *non-degenerate* if $\Delta(X)$ and $\Gamma(\Psi)$ intersect properly. Of course, a morphism of $\mathbb{P}_1$ is non-degenerate if and only if it is not the identity map. We suppose that Φ^n is non-degenerate. Therefore we consider the intersection of $\Delta(X)$ and $\Gamma(\Phi^n)$, denoted by $\Delta(X) \cdot \Gamma(\Phi^n)$, as cycles on the product $X \times X$. For more information about general intersection theory see [16]. Morton and Silverman define the *cycle of n-periodic point of* Φ

$$Z_n(\Phi) := \pi_1(\Delta(X) \cdot \Gamma(\Phi^n))$$

which is the zero-cycle obtained taking the sum of the first coordinates , with their multiplicities, of the intersection of $\Delta(X)$ and $\Gamma(\Phi)$. Therefore, denoting with $a_P(\Phi, n)$ the above multiplicity of a point P, it follows that

$$Z_n(\Phi) = \sum_{P\in X} a_P(\Phi, n)P.$$

For all $P \in X$, it is clear that $a_P(\Phi, n) \geq 0$ and $a_P(\Phi, n) \geq 1$ if and only if P is a n-periodic point for Φ. We define the *cycle of formal n-periodic points of* Φ in the following way:

$$Z^*_n(\Phi) = \sum_{d|n} \mu\left(\frac{n}{d}\right) Z_d(\Phi), \tag{1.15}$$

where μ is the Möbius function. Of course it contains all the primitive n-periodic points of Φ but it can also contain non primitive n-periodic points. For example, see $Z^*_2(\Phi)$ with $\Phi([X : Y]) = [X^2 - XY : Y^2]$. From the definition it is not clear that $Z^*_n(\Phi)$ is an effective zero-cycle. Namely, writing

$$Z^*_n(\Phi) = \sum_{P\in X} a^*_P(\Phi, n)P,$$

it is not clear if $a^*_P(\Phi, n) \geq 0$ for all $P \in X$. Morton and Silverman conjectured that:

Conjecture 1.1. *Let $\Phi\colon X \to X$ be a morphism of a non-singular projective variety X to itself, and suppose that Φ^n is non-degenerate. Then the cycle $Z^*_n(\Phi)$ of formal n-periodic points for Φ is an effective zero cycle.*

They proved this conjecture when Φ is an automorphism of a n-dimensional projective space [23, Theorem 2.1.] and when X has dimension 1 and Φ is a morphism of degree ≥ 2 [23, Proposition 3.2.]. Now we prove this last result by giving the same proof contained in [23, §3].

Let X be a smooth curve. If $P \in X$ is a fixed point for a rational map Ψ, then it defines a map from the cotangent space of X at P to itself

$$(\Psi)^*\colon \Omega_P(X) \to \Omega_P(X).$$

Since $\Omega_P(X)$ is one dimensional, $(\Psi)^*$ is the multiplication by a scalar which is denoted by $(\Psi)'(P)$. In the case $X = \mathbb{P}_1$, for every rational map $\Psi\colon \mathbb{P}_1 \to \mathbb{P}_1$, associating in the canonical way the rational function $\psi \in K(z)$, it results that $(\Psi)'(P) = (\psi)'(P)$, for each point P different from the point at infinity $[1 : 0]$.

In the theory of dynamical system $(\psi)'(P)$ is called the *multiplier* of Φ at P. We have committed an abuse of notation because we have used P to denote a point of $\mathbb{P}_1(K)$ and the relative rational number of K. It is clear that this is not a problem if $P \neq [1:0]$. Otherwise if $P = [1:0]$ we take $\omega = 1/z$ a local uniformizing parameter for z near ∞. Then the derivative of $\omega \mapsto 1/\psi(1/\omega)$ at $\omega = 0$ is equal to limit of $1/\psi'(z)$ as $z \to \infty$. For example for every $c \in K^*$, if $\psi(z) = cz$ then ∞ is a fixed point for ψ with multiplier $1/c$.

Lemma 1.2 (Lemma 3.4 [23]). *Let K be a field, let X/K be a smooth projective curve, and let $\Phi\colon X \to X$ be a non-constant morphism defined over K such that Φ^n is non degenerate. Suppose that $P \in X$ is a fixed point of Φ.*

(a) $a_P(\Phi, n) \geq a_P(\Phi, 1)$ for all $n \geq 1$.

(b) $a_P(\Phi, n) > a_P(\Phi, 1)$ if and only if one of the following two conditions is true:

(i) $a_P(\Phi, 1) = 1$ and $\Phi'(P)^n = 1$.

(ii) $a_P(\Phi, 1) \geq 2$ and $n = 0$ in K, in which case $a_P(\Phi, n) \geq 2a_P(\Phi, 1) - 1$.

Proof. To ease notation, we denote $a = a_P(\Phi, 1)$. Of course $a > 0$ since P is a fixed point of Φ. Let $\mathscr{O}_P$ be the ring of regular functions at P. Let $z \in \mathscr{O}_P$ be a uniformizer at P (i.e. z vanishes to exact order one at P). Since P is a periodic point for Φ and a is the intersection index of $\Delta(X)$ and $\Gamma(\Phi)$ at the point (P, P), we can write

$$z \circ \Phi = z + z^a g \tag{1.16}$$

where $g \in \mathscr{O}_P$ with $g(P) \neq 0$. Note that this holds, locally around P, since non-degeneracy of Φ^n which tells us that $z \circ \Phi \neq z$. we shall write $O(z^k)$ to indicate a function that vanishes to order at least k at P. In this way (1.16) becomes $z \circ \Phi = z + O(z^a)$ and by induction on i we deduce that

$$z \circ \Phi^i = z + O(z^a) \tag{1.17}$$

for all $i \geq 1$. In particular for n

$$a_P(\Phi, n) = \mathrm{ord}_P(z \circ \Phi^n - z) \geq a = a_P(\Phi, 1)$$

which proves the part (a).

Now we prove part (b), beginning with the case $a_P(\Phi, 1) = 1$. Morton and Silverman, with the following argument, relate the value of $a_P(\Phi, n)$ to the value of $(\Phi'(P))^n$. By the assumption $a_P(\Phi, 1) = 1$ there exists a function $G \in \mathscr{O}_P$

such that $z \circ \Phi = zG$ and $G(P) \neq 1$. Since z is a uniformizer at P, with an easy calculation we get to

$$\Phi'(P) = G(P).$$

By induction on n it results that

$$z \circ \Phi^n = z \prod_{i=0}^{n-1} G \circ \Phi^i.$$

Since P is a periodic point for Φ we have that

$$\prod_{i=0}^{n-1} G \circ \Phi^i(P) = G(P)^n.$$

By the last three identities

$$\left(\frac{z \circ \Phi^n - z}{z}\right)(P) = \left(\prod_{i=0}^{n-1} G \circ \Phi^i(P)\right) - 1 = G(P)^n - 1 = \Phi'(P)^n - 1.$$

Therefore $a_P(\Phi, n) \geq 2$ if and only if $\Phi'(P)^n = 1$. This proves Lemma 1.2 in the case when $a_P(\Phi, 1) = 1$.

Now, let $a_P(\Phi, 1) = a \geq 2$, hence $2a - 1 > a$. From (1.17), by linearity, it follows that for all power series, in particular for g

$$g \circ \Phi^i = g + O(z^a). \tag{1.18}$$

Using (1.16) and (1.18), by induction on n it results that

$$\begin{aligned} z \circ \Phi^n &= z + z^a \sum_{i=0}^{n-1} g \circ \Phi^i + O(z^{2a-1}) \\ &= z + nz^a g + O(z^{2a-1}). \end{aligned}$$

Therefore

$$a_P(\Phi, n) = \operatorname{ord}_P(z \circ \Phi^n - z) = \operatorname{ord}_P(nz^a g + O(z^{2a-1}))$$

which is equal to a if and only if $n \neq 0$ in K. If $n = 0$ in K then $a_P(\Phi, n) \geq 2a - 1$.

□

At this point we are ready to show the proof of Proposition 3.2 of [23] which proves Conjecture 1.1 when X is a curve and exactly states when $a_P^*(\Phi, n) > 0$.

Proposition 1.3 (Proposition 3.2 [23])**.** *Let K, X, Φ be as in Lemma 1.2. Fix a point $P \in X$, and define integers m, p, r by*

m =the minimal period of P for Φ (set $m = \infty$ if P is not a periodic point of Φ),

p =the characteristic of K,

r =the multiplicative period of $(\Phi^m)'(P)$ in K^*
(set $r = \infty$ if $m = \infty$ or if $(\Phi^m)'(P)$ is not a root of unity).

Then

(a) $a^*_P(\Phi, n) \geq 0$ for all $n \geq 1$.

(b) Let $n \geq 1$. Then $a^*_P(\Phi, n) \geq 1$ if and only if one of the following three conditions is true:

(i) $n = m$.

(ii) $n = mr$. If $r = 1$, then $a^*_P(\Phi, n) \geq 2$.

(iii) $n = p^e mr$ for some $e \geq 1$, in which case $a^*_P(\Phi, n) \geq 2^{e-1}(a_P(\Phi, mr) - 1)$.

Proof. Of course $a_P(\Phi, n) \geq 1$ if and only if $m|n$. Therefore if m does not divide n then for all integers $d|n$ $\Phi^d(P) \neq P$, hence $a_P(\Phi, d) = 0$ and $a^*_P(\Phi, n) = 0$; this concludes the proof in the case in which P is not a n-periodic point.
Now we suppose that m divides n. Let us denote by N the integer n/m. In many parts of Morton and Silverman's proof, they use the previous Lemma 1.2. Therefore they define

$$\Psi = \Phi^m$$

so that P is a fixed point of Ψ and $r = \Psi'(P)$. For all $a, b \in \mathbb{N}$ it is trivial that $a_P(\Phi, ab) = a_P(\Phi^b, a)$. Thus from this last identity we obtain

$$\begin{aligned} a^*_P(\Phi, n) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) a_P(\Phi, d) \\ &= \sum_{d|n,\ m|d} \mu\left(\frac{n}{d}\right) a_P(\Phi, d) \\ &= \sum_{d|(n/m)} \mu\left(\frac{n}{md}\right) a_P(\Phi, md) \\ &= \sum_{d|N} \mu\left(\frac{N}{d}\right) a_P(\Psi, d). \end{aligned} \tag{1.19}$$

Now, before to consider a number of cases, we prove a relation between $\Psi'(P)$ and $a_P(\Psi, 1) = a_P(\Phi, m)$. Using the same notation of Lemma 1.2, being z a uniformizer at P, we obtain that

$$z \circ \Psi = \Psi'(P)z + O(z^2) \quad \text{(Taylor series)}$$

locally around P. Thus

$$a_P(\Psi, 1) = \mathrm{ord}_P(z \circ \Psi - z) = \mathrm{ord}_P\left[(\Psi'(P) - 1)z + O(z^2)\right]$$

which proves that

$$a_P(\Psi, 1) \geq 2 \Leftrightarrow \Psi'(P) = r = 1. \tag{1.20}$$

Case 1: $N = 1$. It happens when $n = m$. From (1.19), since $N = 1$, it follows that $a^*_P(\Phi, n) = a_P(\Psi, 1)$ which is ≥ 1, since P is a fixed point for Ψ. If $r = 1$ then we are in the case (ii). By (1.20) it follows that that $a^*_P(\Phi, n) \geq 2$. This concludes the proof in this case.

Case 2: $r = 1$, $N > 1$ and $N \neq 0$ in K. We are not in any of conditions (i), (ii) and (iii) of part (b) thus we claim that $a^*_P(\Phi, n) = 0$. From $N > 1$, a standard property of Möbius function states that

$$\sum_{d|N} \mu\left(\frac{N}{d}\right) = 0.$$

Since $r = 1$, from (1.20) it follows that $a_P(\Psi, 1) \geq 2$. Furthermore it is clear that every integer $d|N$ is not zero in K. Therefore, applying the part (b) of Lemma 1.2 with Ψ instead of Φ and d instead of n, we deduce that $a_P(\Psi, d) = a_P(\Psi, 1)$ for all $d|N$. Using this last identity in (1.19), by the above property of Möbius function, we see that $a^*_P(\Phi, n) = 0$. This concludes the proof in this case.

Case 3: $r = 1$, $N = 0$ in K. Let e be the positive integer such that $N = p^e M$ with $p \nmid M$. With this notation (1.19) becomes

$$\begin{aligned} a^*_P(\Phi, n) &= \sum_{i=0}^{e} \sum_{d|M} \mu\left(\frac{N}{p^i d}\right) a_P(\Psi, p^i d) \\ &= \sum_{i=0}^{e} \sum_{d|M} \mu\left(\frac{p^{e-i} M}{d}\right) a_P(\Psi, p^i d) \end{aligned} \tag{1.21}$$

Also in this case $r = 1$ so that (1.20) tells us that $a_P(\Psi, 1) \geq 2$. By part (a) of Lemma 1.2 we deduce that $a_P(\Psi, p^i d) \geq a_P(\Psi, 1) \geq 2$ for all exponents $i \geq 0$ and positive integers $d|M$. From this, applying Lemma 1.2 -part (b) with Ψ^{p^i} instead of Φ and d instead of n, we obtain that $a_P(\Psi, p^i d) = a_P(\Psi, p^i)$, since $d \neq 0$ in K. Using in (1.21) this last identity, by multiplicative property of the Möbius function, it results

$$\begin{aligned} a_P^*(\Phi, n) &= \sum_{i=0}^{e} \sum_{d|M} \mu\left(p^{e-i}\right) \mu\left(\frac{M}{d}\right) a_P(\Psi, p^i) \\ &= \left(\sum_{i=0}^{e} \mu(p^{e-i}) a_P(\Psi, p^i)\right)\left(\sum_{d|M} \mu\left(\frac{M}{d}\right)\right) \\ &= \begin{cases} a_P(\Psi, p^e) - a_P(\Psi, p^{e-1}) & \text{if } M = 1 \\ 0 & \text{if } M \geq 2. \end{cases} \end{aligned} \tag{1.22}$$

This proves part (a), since by a trivial application of Lemma 1.2 -part (a) it follows that $a_P(\Psi, p^e) \geq a_P(\Psi, p^{e-1})$.

By (1.22) $a_P^*(\Phi, n) \geq 1$ if and only if $a_P(\Psi, p^e) > a_P(\Psi, p^{e-1})$ and $M = 1$. This last identity is equivalent to $n = p^e m = p^e mr$, therefore now we have only to prove the bound in (iii) of part (b). From $a_P(\Psi^{p^i}, 1) \geq a_P(\Psi, 1) \geq 2$, applying part (ii)-(b) of Lemma 1.2 to the rational map Ψ^{p^i} with p instead of n, we obtain

$$a_P(\Psi, p^{i+1}) = a_P(\Psi^{p^i}, p) \geq 2a_P(\Psi^{p^i}, 1) - 1 = 2a_P(\Psi, p^i) - 1 \text{ for all index } i \in \mathbb{N} \tag{1.23}$$

Using $i + 1$-times (1.23) we prove that

$$a_P(\Psi, p^{i+1}) \geq 2^{i+1}(a_P(\Psi, 1)) - 2^{i+1} + 1. \tag{1.24}$$

From (1.22) and (1.23) with $i = e - 1$ it follows

$$a_P^*(\Phi, n) \geq a_P(\Psi, p^{e-1}) - 1. \tag{1.25}$$

If $e = 1$ the proof is finished. Otherwise using (1.24) with $i = e - 2$ in (1.25) we deduce that

$$a_P^*(\Phi, n) \geq 2^{e-1}(a_P(\Psi, 1) - 1) = 2^{e-1}(a_P(\Phi, mr) - 1).$$

This concludes the proof in this case.

Case 4: $N > 1$ and $a_P(\Psi, N) = 1$. Since P is a fixed point for Ψ, $a_P(\Psi, 1) \geq 1$. Therefore for every $d|N$, from Lemma 1.2 it follows that $1 \leq a_P(\Psi, 1) \leq a_P(\Psi, d) \leq a_P(\Psi, N) = 1$, so that $a_P(\Psi, d) = 1$ for all $d|N$. Substituting this in (1.19) we obtain

$$a_P^*(\Phi, n) = \sum_{d|N} \mu\left(\frac{N}{d}\right) = 0,$$

since $N > 1$ by assumption; this proves part (a) in this case. To prove part (b) we have to show that

$$n \notin \{m, mr, p^e mr\}. \tag{1.26}$$

Since $a_P(\Psi, 1) = 1$ from (1.20) we deduce that $r > 1$. Moreover $n \neq m$ since $N > 1$. It is clear that if $r = \infty$ then (1.26) holds. Otherwise Ψ' is an r-th primitive root of unity. Assume that (1.26) holds, so that $r|N$. By Lemma 1.2 part (a) it follows that

$$a_P(\Psi, N) \geq a_P(\Psi, r).$$

Furthermore, by Lemma 1.2 part (b)-(i), applied to Ψ instead of Φ and r instead of n, we have that

$$a_P(\Psi, r) > a_P(\Psi, 1) = 1.$$

The two last inequality state that $a_P(\Psi, N) > 1$ which contradicts the assumption $a_P(\Psi, N) = 1$. This concludes the proof in this case.

Case 5: $r > 1$, $N > 1$ and $a_P(\Psi, N) \geq 2$. By the assumption $r > 1$ (1.20) states that $a_P(\Psi, 1) = 1$. From $a_P(\Psi, N) \geq 2$ it follows that $a_P(\Psi, N) > a_P(\Psi, 1) = 1$, so that Lemma 1.2 part (i)-(b) tells us that $\Psi'(P)$ is an N-th root of unity. Hence, since by hypothesis $\Psi'(P)$ is a primitive r-th root of unity, it results that $r|N$. Let

$$N = rM \text{ and } \Lambda = \Psi^r.$$

We prove this case by proving that Proposition 1.3 holds for Λ and M instead of Φ and n respectively. Indeed, since $a_P(\Psi, 1) = 1$ and $(\Psi'(P))^r = 1$, we can apply Lemma 1.2, with Ψ and r instead of Φ and n respectively, obtaining

$$a_P(\Lambda, 1) = a_P(\Psi, r) \geq 2 \quad \text{and} \quad a_P(\Psi, d) = 1 \text{ if } r \nmid d. \tag{1.27}$$

Repeating the argument which gives (1.20) with Λ instead of Ψ we see that $\Lambda'(P) = 1$. Denoting by $r(\Lambda)$ the period of $\Lambda'(P)$ in K^* we have that $r(\Lambda) = 1$. In this way it results that Λ falls into one of the case 1, 2, 3 already treated, so that Proposition 1.3 is true for Λ. More precisely, substituting M instead of n, Proposition 1.3 states that $a^*_P(\Lambda, M) \geq 0$ and $a^*_P(\Lambda, M) \geq 1$ if and only if

$$M = 1, \text{ in which case } a_P(\Lambda, M) \geq 2. \tag{1.28}$$

$$M = p^e \text{ for some } e \geq 1, \text{ in which case } a^*_P(\Lambda, M) \geq 2^{e-1}(a_p(\Lambda, 1) - 1). \tag{1.29}$$

Note that in this situation the minimal period of P for Λ and $r(\Lambda)$ are equal to 1. Hence, the case (1.28) represents both the parts (i) and (ii) of Proposition 1.3 and the case (1.29) represents the part (iii).

The next argument gives a relation between $a_P^*(\Phi, n)$ and $a_P^*(\Lambda, M)$. One can rewrite (1.19) in this way:

$$a_P^*(\Phi, n) = \sum_{d|N,\ r\nmid d} \mu\left(\frac{N}{d}\right) a_P(\Psi, d) + \sum_{d|(N/r)} \mu\left(\frac{N}{dr}\right) a_P(\Psi, dr) \tag{1.30}$$

By (1.27)

$$\begin{aligned}\sum_{d|N,\ r\nmid d} \mu\left(\frac{N}{d}\right) a_P(\Psi, d) &= \sum_{d|N,\ r\nmid d} \mu\left(\frac{N}{d}\right) \\ &= \sum_{d|N} \mu\left(\frac{N}{d}\right) - \sum_{d|(N/r)} \mu\left(\frac{N/r}{d}\right) \\ &= \begin{cases} -1 & \text{if } N = r \quad (\text{i.e. } M = 1) \\ 0 & \text{if } N > r \quad (\text{i.e. } M > 1). \end{cases}\end{aligned} \tag{1.31}$$

The other sum, since $M = N/r$, becomes

$$\begin{aligned}\sum_{d|(N/r)} \mu\left(\frac{N}{dr}\right) a_P(\Psi, dr) &= \sum_{d|M} \mu\left(\frac{M}{d}\right) a_P(\Lambda, d) \\ &= a_P^*(\Lambda, M).\end{aligned} \tag{1.32}$$

Substituting (1.31) and (1.32) in (1.30) we obtain

$$a_P^*(\Phi, n) = \begin{cases} a_P^*(\Lambda, M) - 1 & \text{if } M = 1 \\ a_P^*(\Lambda, M) & \text{if } M > 1. \end{cases} \tag{1.33}$$

Using Proposition 1.3, applied to Λ and M as above, (1.33) tells us that $a_P^*(\Phi, n) \geq 0$ so part (a) is proved also in this case.

If $M = 1$ then $n = mr$ and again from (1.28) and (1.33) we deduce that

$$a_P^*(\Phi, n) = a_P^*(\Lambda, M) - 1 \geq 1.$$

Since in this case $r > 1$, it is not necessary to prove that $a_P^*(\Phi, n) \geq 2$.

Suppose now that $M > 1$. If M is not a power of p, then n does not fall in one of the cases listed in part (b). In this situation Proposition 1.3 applied to Λ (see (1.28)(1.29)) tells us that $a_P^*(\Lambda, M) = 0$ and, again from (1.33), we deduce that $a_P^*(\Phi, n) = 0$, as it is stated in part (b). Finally we suppose that $M = p^e$ for some integer e, which is equivalent to $n = p^e mr$. Again from (1.33) and (1.29) it follows that

$$a_P^*(\Phi, n) = a_P^*(\Lambda, M) \geq 2^{e-1}(a_p(\Lambda, 1) - 1)$$

By definition of Λ and Ψ

$$a_P^*(\Phi, n) \geq 2^{e-1}(a_p(\Phi^{mr}, 1) - 1) = 2^{e-1}(a_p(\Phi, mr) - 1).$$

From this the proof of this case is finished as well as the proof of Proposition 1.3. □

Proposition 1.3 is the main tool to prove the bound

$$[12(s+1)\log(5(s+1))]^{8s} \tag{1.34}$$

given by Morton and Silverman for cycle lengths for rational maps with good reduction outside S (recall that $s = |S|$ and $2s \geq [K : \mathbb{Q}]$). In Proposition 1.3 it is required that Φ^n is non-degenerate. In $\mathbb{P}_1(K)$ this condition is simply verified by asking that Φ is not an automorphism of $\mathbb{P}_1(K)$. Therefore, before to prove the bound (1.34), for rational maps of degree ≥ 2, as proved by Morton and Silverman, we present an elementary argument which prove that the bound (1.34) is valid also in the case of automorphisms.

Proposition 1.4. *Let Φ be an automorphism of K. If the orbit of P under Φ is finite, then its cardinality is $\leq 2 + 16s^2$. In particular (1.34) holds.*

Proof. Of course the orbit of P under Φ is finite if and only if P is a periodic point for Φ. If a point of $\mathbb{P}_1(K)$ is a periodic point for $\Phi \in \mathrm{PGL}_2(K)$, with minimal period $n \geq 3$, then Φ^n is the identity automorphism of $\mathbb{P}_1(K)$. In general we prove that if $\Phi \in \mathrm{PGL}_2(K)$ has order n, then

$$n \leq 2 + 4[K : \mathbb{Q}]^2 \leq 2 + 16s^2. \tag{1.35}$$

since $2s \geq [K : \mathbb{Q}]$.

We choose a matrix $A \in \mathrm{GL}_2(K)$ which represents Φ. Since A^n is a scalar matrix, we have that A is conjugated to a diagonal matrix

$$D = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix},$$

where λ and μ belong to an extension L of degree at most 2 of K. The automorphism in $\mathrm{PGL}_2(K)$ defined by D has order n; therefore $\lambda\mu^{-1} \in L$ is an n-th primitive root of unity and $[\mathbb{Q}(\lambda\mu^{-1}) : \mathbb{Q}]$ divides $[L : \mathbb{Q}]$. It is an elementary fact that $[\mathbb{Q}(\lambda\mu^{-1}) : \mathbb{Q}] = \varphi(n)$, where φ is the Euler's function. Thus $\varphi(n) \leq 2[K : \mathbb{Q}]$. Using the rough lower bound $n - 2 \leq \varphi(n)^2$, we prove (1.35). Of course

$$2 + 16s^2 < [12(s+1)\log(5(s+1))]^{8s}$$

holds for every positive integer s. This concludes the proof □

The next theorem shows that the bound (1.34) holds for rational maps of degree ≥ 2; the proof here presented contains some parts of the proofs of [23, Theorem 4.1], [22, Theorem 1.1] and [22, Corollary].

Theorem 1.4. *Let $\Phi \colon \mathbb{P}_1 \to \mathbb{P}_1$ be a rational map defined over K of degree ≥ 2 with good reduction outside S. Let $P \in \mathbb{P}_1(K)$ be a periodic point for Φ with minimal period n.*

(A) Let $\mathfrak{p} \notin S$ and let p be the rational prime contained in $\mathfrak{p}$. Then n has the form $n = n'n''p^e$ for integers $n', n'' \geq 1$ $e \geq 0$ satisfying

$$n' \leq \#K(\mathfrak{p}) + 1 \quad \textit{and} \quad n'' \mid \#K(\mathfrak{p}) - 1.$$

(B)

$$n < [12(s+1)\log(5s+5)]^{8s} \tag{1.36}$$

Proof. For all $\mathfrak{p} \notin S$, let $\tilde{P} \in \mathbb{P}_1(K(\mathfrak{p}))$ be the reduction modulo $\mathfrak{p}$ of P. Of course it is a n-periodic point for $\tilde{\Phi}$. Let L the finite extension of K which contains all the n-periodic points of Φ. L can be K itself. Let $\mathfrak{b}$ a prime ideal of L lying over $\mathfrak{p}$. Of course the reduction modulo $\mathfrak{b}$ of P still is $\tilde{P}$. For every $d|n$ let $\Phi^d([X : Y]) = [F_d(X,Y) : G_d(X,Y)]$ with the usual condition that $F_d, G_d \in K[X,Y]$ are with same degree, with no common factors and such that F_d, G_d have coefficients in $R_\mathfrak{p}$ and that at least one coefficient is in $R_\mathfrak{p}^*$. Since Φ^d has good reduction at $\mathfrak{p}$, $\tilde{\Phi}^d = [\tilde{F}_d(X,Y) : \tilde{G}_d(X,Y)]$ is the rational map associate to Φ^d in Definition 1.1. Let us consider the set of roots with multiplicities of the equation

$$YF_d(X,Y) - XG_d(X,Y) = 0 \quad \text{in } \mathbb{P}_1(L)$$

and the set of roots with multiplicities of the equation obtained by reduction modulo $\mathfrak{b}$ (or equivalently by reduction modulo $\mathfrak{p}$) of the previous one

$$Y\tilde{F}_d(X,Y) - X\tilde{G}_d(X,Y) = 0 \quad \text{in } \mathbb{P}_1(L(\mathfrak{b})).$$

It is easy to see that

$$a_{\tilde{P}}(\tilde{\Phi}, d) = \sum_{i=0}^{k} a_{Q_i}(\Phi, d) \tag{1.37}$$

where the set $\{Q_0, \dots, Q_k\}$ is the set of all the n-periodic points of $\mathbb{P}_1(L)$ for Φ such that their reduction modulo $\mathfrak{b}$ is equal to $\tilde{P}$. Now from the definition of cycle of formal n-periodic points (1.15) it follows

$$\begin{aligned} a^*_{\tilde{P}}(\tilde{\Phi}, n) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) a_{\tilde{P}}(\tilde{\Phi}, d) \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{i=0}^{k} a_{Q_i}(\Phi, d) \quad \text{from (1.37)} \\ &= \sum_{i=0}^{k} \sum_{d|n} \mu\left(\frac{n}{d}\right) a_{Q_i}(\Phi, d) \\ &= \sum_{i=0}^{k} a^*_{Q_i}(\Phi, n). \end{aligned}$$

Since $P \in \{Q_0, \dots, Q_k\}$ and $a^*_P(\Phi, n) = a_P(\Phi, n) > 0$ (since P is a primitive n-periodic point), we have that $a^*_{\tilde{P}}(\tilde{\Phi}, n) > 0$.

Now we apply the part (b) of Proposition 1.3 to $\tilde{\Phi}\colon \mathbb{P}_1 \to \mathbb{P}_1$ defined over $K(\mathfrak{p})$. The integer n' is instead of m the minimal period of $\tilde{P}$, thus $n' \leq |\mathbb{P}_1(K(\mathfrak{p}))| = \#K(\mathfrak{p}) + 1$, and the integer n'' is instead of r; it is the order of an element of the multiplicative group $K(\mathfrak{p})^*$, therefore $n''|(\#K(\mathfrak{p}) - 1)$. This proves the part (A).

Now we prove part (B). Let $\mathfrak{p}_1, \mathfrak{p}_2 \notin S$ be two distinct prime ideals. For all $i \in \{1, 2\}$, let p_i be the rational prime contained in $\mathfrak{p}_i$. Part (A) tells us that

$$n = n'(\mathfrak{p}_i) n''(\mathfrak{p}_i) p_i^{e(\mathfrak{p}_i)}$$

with $n'(\mathfrak{p}_i) \leq \#K(\mathfrak{p}_i) + 1$, $n''(\mathfrak{p}_i)|\#(K(\mathfrak{p}_i) - 1)$ and a suitable integer $e(\mathfrak{p}_i) \geq 0$. Being p_1 and p_2 coprime it follows that

$$n \leq n'(\mathfrak{p}_1) n''(\mathfrak{p}_1) n'(\mathfrak{p}_2) n''(\mathfrak{p}_2) \leq (\#K(\mathfrak{p}_1)^2 - 1)(\#K(\mathfrak{p}_2)^2 - 1).$$

We suppose that $p_2 > p_1$, from $|\#K(\mathfrak{p}_1)| \leq p_i^{[K:\mathbb{Q}]}$ it follows

$$n < p_2^{4[K:\mathbb{Q}]}. \tag{1.38}$$

Since S includes all archimedean places, it contains at most $s - 1$ prime ideals. Therefore we can choose p_2 at most the $(s + 1)$-th rational prime.
Now using in (1.38) the bound given in [1, Theorem 4.7] we obtain (1.36), since $2s \geq [K : \mathbb{Q}]$. □

Chapter 2

Finiteness results for cycles

2.1 Introduction

The main results of this chapter are reproduced in [6]. They are a generalization to rational maps of the theorems proved by Halter-Koch and Narkiewicz in [13] about polynomials which we have briefly described in the introduction of this thesis. In particular, in this chapter we shall prove the following corollary. Recall that in all part of this thesis we use the notation set at the beginning of section §1.2. In particular K is a fixed number field and S a finite set of places of K containing all the archimedean ones.

Corollary 2.1. *Let $P_0, P_1 \in \mathbb{P}_1(K)$ be two given points. The number of inequivalent cycles for rational maps with good reduction outside S which admit P_0, P_1 as consecutive points is finite. Furthermore there exist an uniform bound for this number, which does not depend on the choice of the points P_0, P_1.*

The definition of equivalent cycles is the same as the one given for ordered n-tuples (see Definition 1.2). Note that given two points P_0, P_1, there could exist infinitely many orbits of the form $(P_0, P_1, \dots, P_{n-1})$. In fact if the ordered n-tuple $(P_0, P_1, \dots, P_{n-1})$ is an orbit for a rational map Φ with good reduction outside S, then for all automorphisms of $\mathbb{P}_1(K)$

$$A \in \mathrm{Stab}(\{P_0, P_1\}) = \{M \in \mathrm{PGL}_2(R_S) \mid M(P_0) = P_0, M(P_1) = P_1\}$$

we have that the tuple $(P_0, P_1, \dots, A(P_i), \dots, A(P_{n-1}))$ is an orbit for the rational map $A \circ \Phi \circ A^{-1}$ which still has good reduction outside S. In general if R_S^* is infinite, then $\mathrm{Stab}(\{P_0, P_1\})$ is an infinite group.

Using the definition stated by Halter-Koch and Narkiewicz in [13], we say that two polynomial cycles $(x_0, x_1, \dots, x_{n-1})$ and $(y_0, y_1, \dots, y_{n-1})$ are equivalent if there exist an S-integer $a \in R_S$ and an S-unit $\epsilon \in R_S^*$ such that $y_i = a + \epsilon x_i$, for every index i. The definition of equivalent cycles for rational maps is the canonical generalization of the one just stated for polynomials.

Theorem 2 in [13], applied to the ring of S-integers R_S, states that there exist only finitely many inequivalent cycles in R_S for polynomial maps in $R_S[z]$ of degree ≥ 2. In this chapter (Theorem 2.2) we prove that this result cannot be extended to rational maps with good reduction outside S.

2.2 Preliminaries

To obtain the finiteness results that we will show in the next section we need some preliminary results. The first two are elementary but very important for the proofs shown in the sequel. They are contained in [23] and state:

Proposition 2.1.

$$\delta_\mathfrak{p}(P_1, P_3) \geq \min\{\delta_\mathfrak{p}(P_1, P_2), \delta_\mathfrak{p}(P_2, P_3)\} \text{ *for all* } P_1, P_2, P_3 \in \mathbb{P}_1(K).$$

Proposition 2.2. *Let $\Phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ be a rational map defined over K which has good reduction at the prime ideal $\mathfrak{p}$. Let $P \in \mathbb{P}_1(K)$ be a periodic point for Φ with minimal period n. Then*

(a) $\delta_\mathfrak{p}(\Phi^i(P), \Phi^j(P)) = \delta_\mathfrak{p}(\Phi^{i+k}(P), \Phi^{j+k}(P))$ *for every* $i, j, k \in \mathbb{Z}$

(b) Let $i, j \in \mathbb{Z}$ *such that* $\gcd(i - j, n) = 1$. *Then*

$$\delta_\mathfrak{p}(\Phi^i(P), \Phi^j(P)) = \delta_\mathfrak{p}(\Phi(P), P).$$

For all integers $t < 0$ we take $\Phi^t(P)$ equal to the value $\Phi^{m_t}(P)$ where $m_t \in \mathbb{N}$ is the smaller integer such that $n|(m_t - t)$.

The congruence property used in the papers of Narkiewicz, Halter-Koch and Pezda (see [13], [24], [25], [27]), about polynomials, are generalized to rational maps by Proposition 2.2.

The part (a) of Proposition 2.2 is a simple application of the following Proposition 2.3. We show the proof of this result, presented by Morton and Silverman in [23, Proposition 5.2], because this represents the fundamental congruence property, concerning the rational maps with good reduction outside S, used in this thesis.

Proposition 2.3. *Let $\Phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ be a rational map defined over K. Then for all prime ideals $\mathfrak{p}$ of good reduction for Φ*

$$\delta_{\mathfrak{p}}(\Phi(P_1), \Phi(P_2)) \geq \delta_{\mathfrak{p}}(P_1, P_2) \quad \textit{for all } P_1, P_2 \in \mathbb{P}_1(K).$$

Proof. We write $\Phi([X : Y]) = [F(X,Y) : G(X,Y)]$ where $F, G \in R\,[x,y]$ have no common factors and are homogeneous of the same degree. We use the canonical notation for $\mathfrak{p}$-adic absolute value

$$|\alpha|_{\mathfrak{p}} = \exp\left(-v_{\mathfrak{p}}(\alpha)\right). \tag{2.1}$$

We can choose the coefficients of F and G in $R_{\mathfrak{p}}$ such that $|F,G|_{\mathfrak{p}} = 1$. Moreover for every point $P = [x : y] \in \mathbb{P}_1(K)$ we shall choose $x, y \in R_{\mathfrak{p}}$ such that $|x,y|_{\mathfrak{p}} = \max\{|x|_{\mathfrak{p}}, |y|_{\mathfrak{p}}\} = 1$. By our assumption on coefficients of F and G, since Φ has good reduction at $\mathfrak{p}$, it result that $|\mathrm{Res}(F,G)|_{\mathfrak{p}} = 1$. As already observed in (1.5) in the proof of Theorem 1.2, there exist four homogeneous polynomials $h_1, h_2, h_3, h_4 \in R_{\mathfrak{p}}[X,Y]$ of degree equal to $d-1$ such that

$$Fh_1 + Gh_2 = \mathrm{Res}(F,G)X^{2d-1}; \quad Fh_3 + Gh_4 = \mathrm{Res}(F,G)Y^{2d-1}. \tag{2.2}$$

Let $P_i = [x_i : y_i]$ for all $i \in \{1,2\}$; from (2.2) we get

$$\begin{aligned}
|\mathrm{Res}(F,G)|_{\mathfrak{p}} &= |\mathrm{Res}(F,G)x_i^{2d-1}, \mathrm{Res}(F,G)y_i^{2d-1}|_{\mathfrak{p}} && \text{since } |x_i, y_i|_{\mathfrak{p}} = 1 \\
&= |(Fh_1 + Gh_2)(x_i,y_i), (Fh_3 + Gh_4)(x_i,y_i)|_{\mathfrak{p}} && \text{by (2.2)} \\
&\leq \max_{1\leq k\leq 4}\{|h_k(x_i,y_i)|_{\mathfrak{p}}\}|F(x_i,y_i), G(x_i,y_i)|_{\mathfrak{p}} && \text{by triangle inequality} \\
&\leq |h_1,h_2,h_3,h_4|_{\mathfrak{p}}|x_i,y_i|_{\mathfrak{p}}^{d-1}|F(x_i,y_i), G(x_i,y_i)|_{\mathfrak{p}} && \text{by triangle inequality} \\
&\leq |F(x_i,y_i), G(x_i,y_i)|_{\mathfrak{p}} && \text{since } |h_1,h_2,h_3,h_4|_{\mathfrak{p}} \leq 1 \text{ and } |x_i,y_i|_{\mathfrak{p}} = 1
\end{aligned}$$

Using (2.1), from $|\mathrm{Res}(F,G)|_{\mathfrak{p}} = 1$ and the last inequality, we obtain

$$0 = v_{\mathfrak{p}}(\mathrm{Res}(F,G)) \geq \min\{v_{\mathfrak{p}}(F(x_i,y_i)), v_{\mathfrak{p}}(G(x_i,y_i))\} \geq 0 \quad \text{for all } i \in \{1,2\}$$

Thus

$$\delta_{\mathfrak{p}}(\Phi(P_1), \Phi(P_2)) = v_{\mathfrak{p}}(F(x_1,y_1)G(x_2,y_2) - F(x_2,y_2)G(x_1,y_1)) \tag{2.3}$$

Now we consider the polynomial

$$F(X_1,Y_1)G(X_2,Y_2) - F(X_2,Y_2)G(X_1,Y_1) \in R_{\mathfrak{p}}[X_1,Y_1,X_2,Y_2].$$

It is bihomogeneous of bidegree (d, d) and it vanishes identically on the diagonal $X_1Y_2 = X_2Y_1$ in $\mathbb{P}_1 \times \mathbb{P}_1$. Therefore there exists a bihomogeneous polynomial $\Psi \in R_\mathfrak{p}[X_1, Y_1, X_2, Y_2]$ such that the polynomial identity

$$F(X_1, Y_1)G(X_2, Y_2) - F(X_2, Y_2)G(X_1, Y_1) = (X_1Y_2 - X_2Y_1)\Psi(X_1, Y_1, X_2, Y_2) \quad (2.4)$$

holds. Substituting in (2.4) the values x_1, y_1, x_2, y_2, we obtain that

$$\begin{array}{rcll} \delta_\mathfrak{p}(P_1, P_2) & = & v_\mathfrak{p}(x_1y_2 - x_2y_1) & \text{by } |x_1, y_1|_\mathfrak{p} = |x_2, y_2|_\mathfrak{p} = 1 \\ & \leq & v_\mathfrak{p}(F(x_1, y_1)G(x_2, y_2) - F(x_2, y_2)G(x_1, y_1)) & \text{from (2.4)} \\ & = & \delta_\mathfrak{p}(\Phi(P_1), \Phi(P_2)) & \text{from (2.3).} \end{array}$$

□

Actually, [23, Proposition 5.2] states the stronger result: for any non zero prime ideal $\mathfrak{p}$ and for all $P_1, P_2 \in \mathbb{P}_1(K)$

$$\delta_\mathfrak{p}(\Phi(P_1), \Phi(P_2)) \geq \delta_\mathfrak{p}(P_1, P_2) - 2v_\mathfrak{p}(\mathrm{Disc}(\Phi)).$$

But as it was observed at the end of §1.2, Φ has good reduction at $\mathfrak{p}$ if and only if $v_\mathfrak{p}(\mathrm{Disc}(\Phi)) = 0$.

Another important argument which we shall frequently use is the fact that S-unit equations of the type

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 1, \quad (2.5)$$

where $a_i \in K^*$, have only a finite number of non-degenerate solutions

$$(x_1, x_2, \ldots, x_n) \in (R_S^*)^n.$$

A solution is called non-degenerate if no subsum vanishes (i.e. $\sum_{i \in I} a_ix_i \neq 0$ for every nonempty subset $I \subsetneq \{1, 2, \ldots, n\}$).
In other words: the equation $X_1 + X_2 + \ldots + X_n = 1$ has only a finite number of non-degenerate solutions $(X_1, \ldots, X_n) \in K^n$ with $v_\mathfrak{p}(X_i)$ fixed for every index i and for every $\mathfrak{p} \notin S$.

This equation has been widely studied in the literature. For $n = 2$, the first proof of the finiteness of solutions of equation (2.5) is due to C.L. Siegel [32] in the particular case that S contains only the archimedean places. After him, K. Mahler studied the case $K = \mathbb{Q}$ and a generic finite set S of places of $\mathbb{Q}$ containing the archimedean one. Later, in 1960 S. Lang extended Mahler's result to arbitrary fields K of characteristic 0 and solutions in any group $\Gamma \subset K^*$ of finite rank.

A. Baker, by his studies on linear forms in logarithms, gave an effective results with $n = 2$. For a quantitative result see [8] in which J.H. Evertse, studying the case where K is a number field of degree d over $\mathbb{Q}$, found that the number of all solutions is bounded by $\leq 3 \cdot 7^{d+2s}$. Note that this upper bound depends only on $s = \#S$ and $d = [K : \mathbb{Q}]$. Since S includes all archimedean places of K, it is clear that $s \geq d/2$. Hence the Evertse's bound becomes $3 \cdot 7^{4s}$ which depends only on s.

For the general case $n \geq 2$, A. J. van der Poorten and H. P. Schlickewei in [35] and J. H. Evertse in [9] proved independently that the set of solutions is finite. But both proofs are non effective. The best quantitative result is due to J. H. Evertse [11]. He found that the number of all non-degenerate solutions to equation (2.5) is at most $2^{35n^4 s}$.

Now we present two lemmas which are proved applying Siegel's Theorem on S-integral points on curves; the proof of this important result, for example, is contained in [31, Chapter 7]. More precisely, we use the finiteness of S-integral points on elliptic curves, which can be also proved using the S-unit equation Theorem; see [17, Theorem D.8.3].

Lemma 2.1. *Let $D, E \in K^*$ be fixed. Given the equation*

$$y^2 = Du + Ev, \tag{2.6}$$

the set

$$\left\{[u : v : y^2] \in \mathbb{P}_2(K) \mid (u, v, y) \in R_S^* \times R_S^* \times R_S \text{ is a solution of (2.6)}\right\}$$

is finite. Also the subset of R_S^* defined by

$$\left\{\frac{u}{v} \mid u, v \in R_S^* \text{ satisfy (2.6) for a suitable } y \in R_S\right\} \tag{2.7}$$

is finite. The same assertion holds for the set of principal ideals of R_S defined by

$$\{yR_S \mid y \text{ satisfies (2.6) for suitable } u, v \in R_S^*\}. \tag{2.8}$$

Moreover the finiteness of the last set is valid also in the case $DE = 0$.

Proof. Dirichlet unit Theorem states that the group of S-units R_S^* is a finitely generated group of rank equal to $|S| - 1$. From this theorem it is easy to see that there exists a finite set $W \subset R_S^*$ such that for every $u \in R_S^*$ there exist $\bar{u} \in R_S^*$ and $w \in W$ such that $u = w\bar{u}^6$.

Let $DE \neq 0$ and let y be an integer which satisfies (2.6) for suitable $u, v \in R_S^*$; then there exist $\bar{u}, \bar{v} \in R_S^*$ and $w_1, w_2 \in W$ such that

$$y^2 = Dw_1\bar{u}^6 + Ew_2\bar{v}^6. \tag{2.9}$$

Consider the elliptic curve defined by the equation $Y^2 = Dw_1X^3 + Ew_2$; (2.9) tells us that $(\bar{u}^2/\bar{v}^2, y/\bar{v}^3)$ is an S-integral point on the elliptic curve. Now, the finiteness of S-integral points on elliptic curve (Siegel's Theorem) and the finiteness of the set W prove the lemma in this case since

$$\frac{y^2}{v} = \frac{1}{w_2}\left(\frac{y}{\bar{v}^3}\right)^2 \text{ and } \frac{u}{v} = \frac{w_1}{w_2}\left(\frac{\bar{u}^2}{\bar{v}^2}\right)^3. \tag{2.10}$$

If $DE = 0$, e.g. $E = 0$, then it is trivial that $y^2R_S = DR_S$. This concludes the proof. □

Lemma 2.2. *Let $D, E \in K$ and $w \in R_S^*$ be fixed. Given the equation*

$$y^2w = D^2u^2 + DuEv + E^2v^2, \tag{2.11}$$

the set of ideals of R_S defined by

$$\{yR_S \mid (u, v, y) \in R_S^* \times R_S^* \times R_S \text{ is a solution of (2.11)}\}$$

is finite and does not depend on w.

Proof. If $DE = 0$ the lemma is trivial. Therefore we suppose that $DE \neq 0$. Without less of generality we can suppose that D and E are integers. Indeed, if they are not, then we can choose an integer F, depending only on D and E, such that $FD, FE \in R_S$ and replace y^2 with F^2y^2 in (2.11).
Suppose that $(u, v, y) \in R_S^* \times R_S^* \times R_S$ is a solution of (2.11). Denoting by ζ and $\bar{\zeta}$ the primitive third roots of unity, equation (2.11) becomes

$$y^2w = (Du - \zeta Ev)(Du - \bar{\zeta}Ev). \tag{2.12}$$

Of course the elements $(Du - \zeta Ev)$ and $(Du - \bar{\zeta}Ev)$ are algebraic integers of the extension $K(\zeta)/K$ with the property that

$$(Du - \zeta Ev) - (Du - \bar{\zeta}Ev) = (\bar{\zeta} - \zeta)Ev.$$

Let T be the ring of algebraic integers of $K(\zeta)$ and let $\bar{S}$ be the finite set of all places of $K(\zeta)$ which lie over any place of K contained in S. Moreover we can

enlarge $\bar{S}$ to a finite set of places such that the set $T_{\bar{S}}$ of $\bar{S}$-integers in $K(\zeta)$ is a unique factorization domain and such that $(\bar{\zeta}-\zeta)E$ is an element of the set $T_{\bar{S}}^*$ of $\bar{S}$-units in $K(\zeta)$. From this choice of $\bar{S}$ we obtain that $(Du-\zeta Ev)$ and $(Du-\bar{\zeta}Ev)$ are coprime $T_{\bar{S}}$-integers. Therefore by (2.12), after multiplication by a unit, $(Du-\zeta Ev)$ and $(Du-\bar{\zeta}Ev)$ are squares in $T_{\bar{S}}$. For example, let us write $(Du-\zeta Ev)=t\bar{y}^2$ with a suitable $t\in T_{\bar{S}}^*$ and $\bar{y}\in T_{\bar{S}}$. Applying the Lemma 2.1 to the equation $\bar{y}^2=Du/t-\zeta Ev/t$, in particular the finiteness of set (2.7), one easily deduces that there exists a finite set $\mathcal{U}\subset T_{\bar{S}}^*$, such that for every $u,v\in T_{\bar{S}}^*$ which satisfy (2.11) $u/v\in\mathcal{U}$.
Since $R_S^*\subset T_{\bar{S}}^*$ the last statement is true also when we consider $u,v\in R_S^*$. The proof follows by observing that

$$(yR_S)^2=\frac{y^2w}{v^2}R_S=\left(D^2\frac{u^2}{v^2}+DE\frac{u}{v}+E^2\right)R_S$$

□

2.3 Some finiteness results for inequivalent cycles

Given two points $P,Q\in\mathbb{P}_1(K)$ we define the ideal

$$\Im(P,Q):=\prod_{\mathfrak{p}\notin S}\mathfrak{p}^{\delta_\mathfrak{p}(P,Q)}. \tag{2.13}$$

From definition of $\delta_\mathfrak{p}$ it follows that $\Im(P,Q)$ is characterized by the property that $P\equiv Q\ (\mathrm{mod}\ \Im(P,Q))$ and that for every ideal $\Im$ such that $P\equiv Q\ (\mathrm{mod}\ \Im)$ one has $\Im\mid\Im(P,Q)$. To every n-tuple $(P_0,P_1,\dots,P_{n-1})$ we can associate the $(n-1)$-tuple of ideals $(\Im_1,\Im_2,\dots,\Im_{n-1})$ defined by

$$\Im_i:=\prod_{\mathfrak{p}\notin S}\mathfrak{p}^{\delta_\mathfrak{p}(P_0,P_i)}=\Im(P_0,P_i). \tag{2.14}$$

Therefore if the n-tuple $(P_0,P_1,\dots,P_{n-1})$ has good reduction outside S, then the $(n-1)$-tuple $(\Im_1,\Im_2,\dots,\Im_{n-1})$ of ideals defined by (2.14) is equal to $(R_S,\dots,R_S)$. Furthermore if the n-tuples $(P_0,\dots,P_{n-1})$ and $(Q_0,\dots,Q_{n-1})$ are equivalent, then the $(n-1)$-tuples $(\Im_1,\Im_2,\dots,\Im_{n-1})$ of ideals defined by (2.14) coincide.
The Proposition 2.2, in terms of the ideal defined in (2.13), states that for any cycle $(P_0,P_1,\dots,P_{n-1})$, for maps with good reduction outside S, and for all indexes i,k, the ideals $\Im(P_0,P_i)$ and $\Im(P_k,P_{k+i})$ are equal. Moreover if k and n are coprime, then the ideals $\Im(P_0,P_k)$ and $\Im(P_0,P_1)$ are equal.

This section is dedicated to prove the following:

Theorem 2.1. *There exists a finite set $\mathbb{I}_S$ of ideals of R_S with the following property: for every cycle $(P_0, P_1, \dots, P_{n-1})$ for a rational map with good reduction outside S, let $(\mathfrak{I}_1, \mathfrak{I}_2, \dots, \mathfrak{I}_{n-1})$ be the associated $(n-1)$-tuple of ideals; then*

$$\mathfrak{I}_i \mathfrak{I}_1^{-1} \in \mathbb{I}_S$$

for every index $i \in \{1, \dots, n-1\}$.

The proof of Corollary 2.1 will be a direct consequence of Theorem 2.1 by applying the result obtained by Birch and Merriman in 1972 [5]. Another application of Theorem 2.1 will be the following:

Corollary 2.2. *There exists a finite set $\mathcal{N}$ of tuples such that every cycle in $\mathbb{P}_1(K)$, for a rational map with good reduction outside S, can be transformed by an automorphism in $\mathrm{PGL}_2(K)$ in a tuple in $\mathcal{N}$.*

By definition of good reduction for a map, it is clear that any rational map, with good reduction outside S, has good reduction outside every set of places containing S. Therefore we can enlarge S to a finite set $\mathbb{S}$ so that $R_{\mathbb{S}}$ is a P.I.D.. Note that the cardinality of a minimum enlarged set, with the above property, is bounded by $s + h_S - 1$, where h_S is the class number of R_S. To see this suppose that all prime ideals are principal, then it is trivial that R_S is a P.I.D.; otherwise take a prime ideal which is not principal, of course it is contained in an ideal class which is not the trivial one. We add this prime ideal to S, obtaining a larger set S'. It is clear that the new ring $R_{S'}$ has class number $h_{S'} < h_S$; by inductive method it results that to obtain a P.I.D. it suffices to add to S a number of prime ideals $\leq h_S - 1$. Another way to prove this last fact is to apply the "Dirichlet's Theorem"about the uniform distribution of the prime ideals among the ideal classes [20, Chapter 8].

Since $R_{\mathbb{S}}$ is a principal domain, we can adopt the convention that any point $P_i \in \mathbb{P}_1(K)$ will be represented by coprime $\mathbb{S}$-integral homogeneous coordinates $[x_i : y_i]$. By this convention for all prime ideals $\mathfrak{p} \notin \mathbb{S}$ and all points $P_1, P_2 \in \mathbb{P}_1(K)$ it follows that $\delta_{\mathfrak{p}}(P_1, P_2) = v_{\mathfrak{p}}(x_1 y_2 - x_2 y_1)$. Now we prove an elementary lemma which states part *(a)* of Proposition 2.2 in a form which will be useful in the sequel:

Lemma 2.3. *For every cycle $(P_0, P_1, \dots, P_{n-1})$, for rational maps with good reduction outside $\mathbb{S}$, and for every $i, j \in \mathbb{Z}$ there exist an $\mathbb{S}$-unit $u_{j,j+i} \in R_{\mathbb{S}}^*$ such that*

$$(x_j y_{j+i} - x_{j+i} y_j) = (x_0 y_i - x_i y_0) u_{j,j+i}. \tag{2.15}$$

Proof. Part (a) of Proposition 2.2 asserts that, for every prime ideal $\mathfrak{p} \notin \mathbb{S}$ and for every couple of indexes $i, j \in \mathbb{Z}$, we have that $\delta_{\mathfrak{p}}(P_j, P_{j+i}) = \delta_{\mathfrak{p}}(P_0, P_i)$. By the convention assumed on the choice of homogeneous coordinates for points in $\mathbb{P}_1(K)$, the last identity becomes $v_{\mathfrak{p}}(x_j y_{j+i} - x_{j+i} y_j) = v_{\mathfrak{p}}(x_0 y_j - x_j y_0)$. Hence

$$u_{j,j+i} = \frac{x_j y_{j+i} - x_{j+i} y_j}{x_0 y_i - x_i y_0} \in R_{\mathbb{S}}^*$$

which completes the proof □

Lemma 2.4. *For every cycle $(P_0, P_1, \ldots, P_{n-1})$ in $\mathbb{P}_1(K)$, for rational maps with good reduction outside $\mathbb{S}$, and for every prime ideal $\mathfrak{p} \notin \mathbb{S}$ the following properties hold:*

1. *For all indexes $j \in \{0, 1, \ldots, n-1\}, i \not\equiv 0 \pmod n$ we have $\delta_{\mathfrak{p}}(P_j, P_{j+i}) \geq \delta_{\mathfrak{p}}(P_0, P_1)$, or equivalently*

$$C_i := \frac{x_0 y_i - x_i y_0}{x_0 y_1 - x_1 y_0} \in R_{\mathbb{S}} \tag{2.16}$$

and

$$x_j y_{j+i} - x_{j+i} y_j = C_i u_{j,j+i} (x_0 y_1 - x_1 y_0), \tag{2.17}$$

where $u_{j,j+i} \in R_{\mathbb{S}}^*$.

2. *Let $P_0 = [x_0 : y_0]$ and $P_1 = [x_1 : y_1]$ be the first and the second point of the cycle $(P_0, P_1, \ldots, P_{n-1})$. The matrix $A \in \mathrm{GL}_2(K)$*

$$A = \begin{pmatrix} \dfrac{-y_0}{x_0 y_1 - x_1 y_0} & \dfrac{x_0}{x_0 y_1 - x_1 y_0} \\ \dfrac{y_1}{x_0 y_1 - x_1 y_0} & \dfrac{-x_1}{x_0 y_1 - x_1 y_0} \end{pmatrix} \tag{2.18}$$

maps the vector (x_0, y_0) to $(0, 1)$ and the vector (x_1, y_1) to $(1, 0)$. For any index k, if $(\bar{x}_k, \bar{y}_k)^t = A(x_k, y_k)^t$, then for all indexes $j \in \{0, 1, \ldots, n-1\}, i \not\equiv 0$ $\pmod n$ the following identities hold

$$\bar{x}_j \bar{y}_{j+i} - \bar{x}_{j+i} \bar{y}_j = -C_i u_{j,j+i}, \tag{2.19}$$

where $u_{j,j+i}$ is the $\mathbb{S}$-unit defined in part 1. Furthermore for every index $k > 1$

$$(\bar{x}_k, \bar{y}_k) = (C_k, -C_{k-1} u_{1,k}). \tag{2.20}$$

3. *If* $i, j > 0$ *are coprime integers, then*

$$\min\{\delta_{\mathfrak{p}}(P_0, P_i), \delta_{\mathfrak{p}}(P_0, P_j)\} = \delta_{\mathfrak{p}}(P_0, P_1) \tag{2.21}$$

and

$$\min\{v_{\mathfrak{p}}(C_i), v_{\mathfrak{p}}(C_j)\} = 0 \tag{2.22}$$

for every prime ideal $\mathfrak{p} \notin \mathbb{S}$.

Proof. 1. The $\mathfrak{p}$-adic distance satisfies the triangle inequality (Proposition 2.1). Therefore it follows that

$$\begin{array}{rcll} \delta_{\mathfrak{p}}(P_j, P_{j+i}) & \geq & \min\{\delta_{\mathfrak{p}}(P_j, P_{j+1}), \dots, \delta_{\mathfrak{p}}(P_{j+i-1}, P_{j+i})\} & \\ & = & \delta_{\mathfrak{p}}(P_0, P_1) & \text{by Proposition 2.2} \end{array} \tag{2.23}$$

for all indexes $j \in \{0, 1, \dots, n-1\}, i \not\equiv 0 \pmod n$. Thus, by the choice of coprime homogeneous coordinates for every points of $\mathbb{P}_1(K)$ we have that

$$\begin{array}{rcll} v_{\mathfrak{p}}(x_0 y_i - x_i y_0) & = & \delta_{\mathfrak{p}}(P_0, P_i) = \delta_{\mathfrak{p}}(P_j, P_{j+i}) & \text{by Proposition 2.2} \\ & \geq & \delta_{\mathfrak{p}}(P_0, P_1) & \text{by (2.23)} \\ & = & v_{\mathfrak{p}}(x_0 y_1 - x_1 y_0) & \end{array}$$

so that (2.16) is proved. Note that $C_1 = 1$. The identity (2.17) follows from (2.15) and (2.16). Of course if $j = 0$ then $u_{j,j+i} = 1$ for all positive indexes i.

2. Let A be the matrix defined in (2.18). It is an easy computation to see that $A(x_0, y_0)^t = (0, 1)^t$ and $A(x_1, y_1)^t = (1, 0)^t$. For every index k, denoting by $(\bar{x}_k, \bar{y}_k)^t = A(x_k, y_k)^t$, it follows that

$$\bar{x}_j \bar{y}_{j+i} - \bar{x}_{j+i} \bar{y}_j = \det(A)(x_j y_{j+i} - x_{j+i} y_j) = -\frac{x_j y_{j+i} - x_{j+i} y_j}{x_0 y_1 - x_1 y_0}$$

for all indexes $j \in \{0, 1, \dots, n-1\}, i \not\equiv 0 \pmod n$. Using (2.17) in the last identity we obtain (2.19).

Now, we consider (2.19) with $j = 0, i = k$ obtaining

$$-C_k = \bar{x}_0 \bar{y}_k - \bar{x}_k \bar{y}_0 = -\bar{x}_k,$$

since $(x_0, y_0) = (0, 1)$ and $u_{0,k} = 1$ for all indexes k. Considering (2.19) with $j = 1, i = k - 1$ we obtain

$$-C_{k-1} u_{1,k} = \bar{x}_1 \bar{y}_k - \bar{x}_k \bar{y}_1 = \bar{y}_k$$

since $(x_1, y_1) = (1, 0)$. This concludes the proof of (2.20).

3. Since i and j are coprime, there exist $c, d \in \mathbb{Z}$ such that $ci + dj = 1$. Suppose that $dj < 0$. Of course, the case $ci < 0$ is similar.

$$\begin{aligned} \delta_{\mathfrak{p}}(P_0, P_1) &\leq \min\{\delta_{\mathfrak{p}}(P_0, P_{ci}), \delta_{\mathfrak{p}}(P_0, P_{-dj})\} && \text{by part 1} \\ &\leq \delta_{\mathfrak{p}}(P_{ci}, P_{-dj}) && \text{triangle inequality} \\ &= \delta_{\mathfrak{p}}(P_0, P_1) && \text{part (a) of Proposition 2.2} \end{aligned} \tag{2.24}$$

Suppose that $\min\{\delta_{\mathfrak{p}}(P_0, P_{ci}), \delta_{\mathfrak{p}}(P_0, P_{-dj})\} = \delta_{\mathfrak{p}}(P_0, P_{ci})$ (clearly the other case is similar). (2.24) tells us that $\delta_{\mathfrak{p}}(P_0, P_{ci}) = \delta_{\mathfrak{p}}(P_0, P_1)$, hence by part *1*

$$\delta_{\mathfrak{p}}(P_0, P_1) \leq \delta_{\mathfrak{p}}(P_0, P_i) \leq \delta_{\mathfrak{p}}(P_0, P_{ci}) = \delta_{\mathfrak{p}}(P_0, P_1)$$

so that (2.21) follows .
Moreover

$$\begin{aligned} \delta_{\mathfrak{p}}(P_0, P_i) &= v_{\mathfrak{p}}(x_0 y_i - x_i y_0) && \text{by choice of coordinates} \\ &= v_{\mathfrak{p}}(C_i) + v_{\mathfrak{p}}(x_0 y_1 - x_1 y_0) && \text{by (2.17)} \\ &= v_{\mathfrak{p}}(C_i) + \delta_{\mathfrak{p}}(P_0, P_1), \end{aligned}$$

therefore it follows that $v_{\mathfrak{p}}(C_i) = 0$ which proves (2.22). □

Lemma 2.4 states that, for every cycle $(P_0, P_1, \ldots, P_{n-1})$, for rational maps with good reduction outside $\mathbb{S}$, and for every couple of indexes $j \in \{0, 1, \ldots, n-1\}, i \not\equiv 0 \pmod{n}$, the ideal $\mathfrak{I}(P_0, P_1)$ divides the ideal $\mathfrak{I}(P_j, P_{j+i})$. Moreover, for each index $i \in \{2, \ldots, n-1\}$, it allows us to choose some $\mathbb{S}$-integers C_i which generate the ideal $\mathfrak{I}(P_0, P_i) \cdot \mathfrak{I}(P_0, P_1)^{-1}$. Furthermore, it states that if i, j are coprime, then the greatest common divisor of $\mathfrak{I}(P_0, P_i)$ and $\mathfrak{I}(P_0, P_j)$ is $\mathfrak{I}(P_0, P_1)$.

Lemma 2.5. *Let $(P_0, P_1, \ldots, P_{n-1})$ be a cycle, for rational maps with good reduction outside $\mathbb{S}$, and let $i, j \in \mathbb{Z}$; then*

$$L_{i,j} := \frac{x_0 y_{i\cdot j} - x_{i\cdot j} y_0}{x_0 y_j - x_j y_0} \in R_{\mathbb{S}}. \tag{2.25}$$

Moreover, let i, j be fixed coprime integers. Considering only cycles for rational maps with good reduction outside $\mathbb{S}$, if the set of principal ideals generated by the possible values of $L_{i,j}$ is finite, then also the set of principal ideals generated by the possible values of C_i is finite, where C_i is the $\mathbb{S}$-integer defined in (2.16).

Proof. Let $(P_0, P_1, \ldots, P_{n-1})$ be a cycle for a rational map Φ with good reduction outside $\mathbb{S}$. We prove (2.25) applying the first part of Lemma 2.4 to ordered tuple $(P_0, P_j, P_{2j}, \ldots)$, which is a cycle for the rational map Φ^j.

To prove the second part we suppose that $i, j \in \mathbb{Z}$ are coprime. By (2.25) and (2.16)

$$x_0 y_{i\cdot j} - x_{i\cdot j} y_0 = L_{i,j} C_j (x_0 y_1 - x_1 y_0)$$

and

$$x_0 y_{i\cdot j} - x_{i\cdot j} y_0 = L_{j,i} C_i (x_0 y_1 - x_1 y_0),$$

therefore it follows that $L_{i,j} C_j = L_{j,i} C_i$.
By the last identity, from (2.22) in Lemma 2.4 it follows that $v_{\mathfrak{p}}(C_i) \leq v_{\mathfrak{p}}(L_{i,j})$, for every $\mathfrak{p} \notin S$. This tells us that the principal ideal $C_i R_{\mathbb{S}}$ divides $L_{i,j} R_{\mathbb{S}}$. Therefore the finiteness of principal ideals generated by the possible values of $L_{i,j}$ gives the finiteness of principal ideals generated by the possible values of C_i. □

The following lemma is maybe the most important preliminary result useful to prove Theorem 2.1. In its proof we use all previous lemma which we have proved in this chapter.

Lemma 2.6. *Let $n \geq 3$ and $C_2(P_0, P_1, \ldots, P_{n-1})$ be the integer associated to a cycle $(P_0, P_1, \ldots, P_{n-1})$ as defined in (2.16) of Lemma 2.4. The set of principal ideals of $R_{\mathbb{S}}$*

$$\left\{ C_2 R_{\mathbb{S}} \;\middle|\; \begin{array}{l} C_2 = C_2(P_0, P_1, \ldots, P_{n-1}) \textit{ where } (P_0, P_1, \ldots, P_{n-1}) \textit{ is a} \\ \textit{cycle for a rational map with good reduction outside } \mathbb{S} \end{array} \right\} \tag{2.26}$$

is finite.

Proof. In this proof we use the same notation of Lemma 2.4.

Let $(P_0, P_1, \ldots, P_{n-1})$ be a cycle for a rational map with good reduction outside $\mathbb{S}$. For all positive integers i coprime with n

$$\begin{array}{rcll} \delta_{\mathfrak{p}}(P_1, P_0) & = & \min\{\delta_{\mathfrak{p}}(P_i, P_0), \delta_{\mathfrak{p}}(P_n, P_0)\} & \text{by (2.21)} \\ & = & \min\{\delta_{\mathfrak{p}}(P_i, P_0), \delta_{\mathfrak{p}}(P_0, P_0)\} & \text{since } P_n = \Phi^n(P_0) = P_0 \\ & = & \delta_{\mathfrak{p}}(P_i, P_0) & \text{since } \delta_{\mathfrak{p}}(P_0, P_0) = \infty \end{array} \tag{2.27}$$

This proves that the $\mathbb{S}$-integer C_i defined in (2.16) is a $\mathbb{S}$-unit. Therefore if n is an odd number, then C_2 generates always the trivial ideal $R_{\mathbb{S}}$; so that the lemma is proved in this case.

By Lemma 2.4-Part 2, every cycle is mapped by the automorphism defined in (2.18) to the following ordered n-tuple of vectors of K^2

$$(0,1);(1,0);\ldots;(\bar{x}_i,\bar{y}_i)=(C_i,-C_{i-1}u_{1,i});\ldots;(C_{n-1},-C_{n-2}u_{1,n-1})\,.$$

Suppose now that $3\nmid n$, (2.27) tells us that C_3 is an $\mathbb{S}$-unit. The identity (2.19) of Lemma 2.4 applied with $i=1$, $j=2$ becomes

$$-u_{2,3}=\bar{x}_2\bar{y}_3-\bar{x}_3\bar{y}_2=-C_2^2u_{1,3}+C_3u_{1,2}$$

hence

$$C_2^2=\frac{C_3u_{1,2}}{u_{1,3}}+\frac{u_{2,3}}{u_{1,3}}.$$

Now we can apply Lemma 2.1, with $u=C_3u_{1,2}/u_{1,3}$, $v=u_{2,3}/u_{1,3}$, $D=E=1$ and $C_2=y$ obtaining that the set (2.26) is finite.

Let us suppose now that $6|n$. Thus we can write $n=2\cdot3^k\cdot m$ with $m\geq1$ and $3\nmid m$. If $m>1$ and $(P_0,P_1,\ldots,P_{n-1})$ is a cycle for a rational map Φ with good reduction outside $\mathbb{S}$, then the n-tuple $(P_0,P_{3^k},\ldots,P_{(2m-1)3^k})$ is a cycle for the rational map Φ^{3^k} which still has good reduction outside $\mathbb{S}$. Let

$$L_{2,3^k}=\frac{x_0y_{2\cdot3^k}-x_{2\cdot3^k}y_0}{x_0y_{3^k}-x_{3^k}y_0}.$$

The $\mathbb{S}$-integer $L_{2,3^k}$ is “the coefficient C_2”of the cycle $(P_0,P_{3^k},\ldots,P_{(2m-1)3^k})$ which has length equal to $2m\geq4$ which is coprime with 3. Thus by the reasoning did in the previous case ($3\nmid n$) we deduce that the set of principal ideals of $R_{\mathbb{S}}$ generated by $L_{2,3^k}$ is finite. Now we apply Lemma 2.5 with $i=2$ and $j=3^k$ to obtain the finiteness of the set (2.26) in this case.

If $m=1$, we are considering the last case $n=2\cdot3^k$. We first reduce to the case $k=1$. In other words we suppose that lemma holds for $n=6$. If $k>1$ we consider the cycle

$$(P_0,P_{3^{k-1}},\ldots,P_{5\cdot3^{k-1}})\tag{2.28}$$

which has length 6. By our assumption, about the validity of lemma with $n=6$, we deduce the finiteness of the ideals generated by $L_{2,3^{k-1}}$, i.e. “the coefficient C_2”of the cycle (2.28). Also in this situation we apply Lemma 2.5 with $i=2$ and $j=3^{k-1}$ obtaining that the set (2.26) is finite.

Therefore let $n=6$. By Lemma 2.4-Part 2, any 6-tuple $(P_0,P_1,P_2,P_3,P_4,P_5)$ which is cycle for a rational map of good reduction outside $\mathbb{S}$, by the matrix defined in (2.18), is sent to the following ordered 6-tuple of vectors of K^2

$$(0,1);(1,0);(C_2,-u_{1,2});(C_3,-C_2u_{1,3});(C_4,-C_3u_{1,4});(C_5,-C_4u_{1,5})$$

with $u_{1,i} \in R_S^*$ for every $i \in \{2,3,4,5\}$.
By Lemma 2.3 the identities $C_4 = C_2 u_{0,4}$ and $C_5 = u_{0,5}$ hold for suitable $u_{0,4}, u_{0,5} \in R_S^*$. We rewrite the above 6-tuple as

$$(0,1); (1,0); (C_2, -u_{1,2}); (C_3, -C_2 u_{1,3}); (C_2 u_{0,4}, -C_3 u_{1,4}); (u_{0,5}, -C_2 u_{0,4} u_{1,5})$$

Considering this 6-tuple, the identity (2.19) of Lemma 2.4 with $j = 2$ and $i = 2$ becomes

$$-C_2 C_3 u_{1,4} + C_2 u_{1,2} u_{0,4} = -C_2 u_{2,4} \quad \text{where } u_{2,4} \in R_{\mathbb{S}}^*$$

by dividing the left and right terms by $-C_2$ we get to

$$C_3 u_{1,4} - u_{1,2} u_{0,4} = u_{2,4}. \tag{2.29}$$

The identity (2.19) with $j = 2$ and $i = 3$ becomes

$$-C_2^2 u_{0,4} u_{1,5} + u_{1,2} u_{0,5} = -C_3 u_{2,5} \tag{2.30}$$

and with $j = 4$ and $i = 1$

$$-C_2^2 u_{0,4}^2 u_{1,5} + C_3 u_{1,4} u_{0,5} = -u_{4,5}. \tag{2.31}$$

From (2.29) we deduce

$$C_3 = u_{1,2} u_{0,4} u_{1,4}^{-1} + u_{2,4} u_{1,4}^{-1}. \tag{2.32}$$

Now multiplying (2.30) by $u_{0,4}$ and deducting (2.31) we obtain

$$u_{0,4} u_{1,2} u_{0,5} + C_3 u_{2,5} u_{0,4} - C_3 u_{1,4} u_{0,5} = u_{4,5};$$

by replacing C_3 with the right term of (2.32) in this last identity we obtain the following $\mathbb{S}$-unit equation:

$$\frac{u_{1,2} u_{0,4}^2 u_{2,5}}{u_{4,5} u_{1,4}} + \frac{u_{2,4} u_{0,4} u_{2,5}}{u_{4,5} u_{1,4}} - \frac{u_{2,4} u_{0,5}}{u_{4,5}} = 1. \tag{2.33}$$

Suppose that the equation (2.33) has no vanishing subsums. By the $\mathbb{S}$-unit equation Theorem, there exist only finitely many possible values for the ratios

$$\frac{u_{1,2} u_{0,4}^2 u_{2,5}}{u_{4,5} u_{1,4}}; \; \frac{u_{2,4} u_{0,4} u_{2,5}}{u_{4,5} u_{1,4}}; \; \frac{u_{2,4} u_{0,5}}{u_{4,5}}.$$

From (2.32) it follows that

$$C_3 = \frac{u_{4,5}}{u_{0,4}u_{2,5}}\left(\frac{u_{1,2}u_{0,4}^2u_{2,5}}{u_{4,5}u_{1,4}} + \frac{u_{2,4}u_{0,4}u_{2,5}}{u_{4,5}u_{1,4}}\right) \tag{2.34}$$

therefore the set of principal ideals of $R_{\mathbb{S}}$ generated by C_3 is finite. Hence, there exists a finite set C such that $C_3w \in C$ for a suitable $w \in R_{\mathbb{S}}^*$. From (2.30) we deduce

$$C_2^2 = C_3w\frac{u_{2,5}}{wu_{0,4}u_{1,5}} + \frac{u_{1,2}u_{0,5}}{u_{0,4}u_{1,5}}. \tag{2.35}$$

By finiteness of the set C, applying Lemma 2.1 with $C_2 = y$, $D = C_3w$, $E = 1$, $u = u_{2,5}/(wu_{0,4}u_{1,5})$ and $v = (u_{1,2}u_{0,5})/(u_{0,4}u_{1,5})$ we deduce that the set (2.26) is finite.

The equation (2.34) also states that subsum of (2.33)

$$\frac{u_{1,2}u_{0,4}^2u_{2,5}}{u_{4,5}u_{1,4}} + \frac{u_{2,4}u_{0,4}u_{2,5}}{u_{4,5}u_{1,4}}$$

cannot be equal to 0 since $n = 6$.

Let us consider another vanishing subsum in (2.33)

$$\frac{u_{1,2}u_{0,4}^2u_{2,5}}{u_{4,5}u_{1,4}} - \frac{u_{2,4}u_{0,5}}{u_{4,5}} = 0$$

which is equivalent to

$$\frac{u_{2,4}u_{0,4}u_{2,5}}{u_{4,5}u_{1,4}} = 1$$

since (2.33) holds. By these last two identities it follows that

$$u_{1,2}u_{0,4}u_{0,5} = \frac{u_{2,4}^2u_{0,5}^2}{u_{4,5}}. \tag{2.36}$$

Now multiplying (2.29) by $u_{0,5}$ we deduce that

$$C_3u_{1,4}u_{0,5} = u_{1,2}u_{0,4}u_{0,5} + u_{2,4}u_{0,5}.$$

Therefore from this last identity and (2.31) we obtain

$$C_2^2 = \frac{1}{u_{0,4}^2u_{1,5}}(u_{1,2}u_{0,4}u_{0,5} + u_{2,4}u_{0,5} + u_{4,5}). \tag{2.37}$$

By replacing $u_{1,2}u_{0,4}u_{0,5}$ in (2.37) with the right term of (2.36) it results

$$C_2^2 = \frac{1}{u_{0,4}^2u_{1,5}u_{4,5}}(u_{2,4}^2u_{0,5}^2 + u_{2,4}u_{0,5}u_{4,5} + u_{4,5}^2); \tag{2.38}$$

Now we apply Lemma 2.2 with $D = E = 1$, $u = u_{2,4}u_{0,5}$, $v = u_{4,5}$, obtaining the finiteness of the set (2.26).

At last we consider the case

$$\frac{u_{2,4}u_{0,4}u_{2,5}}{u_{4,5}u_{1,4}} - \frac{u_{2,4}u_{0,5}}{u_{4,5}} = 0 \tag{2.39}$$

which is equivalent to

$$\frac{u_{1,2}u_{0,4}^2u_{2,5}}{u_{4,5}u_{1,4}} = 1 \tag{2.40}$$

since (2.33) holds. By dividing both terms of (2.40) by $u_{1,2}u_{0,4}$ we obtain

$$\frac{u_{0,4}u_{2,5}}{u_{4,5}u_{1,4}} = \frac{1}{u_{1,2}u_{0,4}}. \tag{2.41}$$

By replacing in (2.39) $(u_{0,4}u_{2,5})/(u_{4,5}u_{1,4})$ with the right term of (2.41) we obtain

$$\frac{u_{2,4}}{u_{1,2}u_{0,4}} - \frac{u_{2,4}u_{0,5}}{u_{4,5}} = 0$$

which is equivalent to $u_{1,2}u_{0,4}u_{0,5} = u_{4,5}$. From this last identity and (2.37) we obtain

$$C_2^2 = \frac{u_{2,4}u_{0,5}}{u_{0,4}^2u_{1,5}} + 2\frac{u_{4,5}}{u_{0,4}^2u_{1,5}}.$$

Lemma 2.1, applied with $C_2 = y$, $D = 1$, $E = 2$, $u = (u_{2,4}u_{0,5})/(u_{0,4}^2u_{1,5})$ and $v = u_{4,5}/(u_{0,4}^2u_{1,5})$ provides the finiteness of the set (2.26) also in this last case. □

This proof is not effective since we have used the $\mathbb{S}$-unit equation Theorem in three variables. In particular this proof does not provide an effective method to find the set of possible values for $D = C_3w$ in (2.35), therefore we cannot determine the set (2.26), either.

Now we introduce a notation which will simplify the next statements and proofs.

For any integer $i \in \mathbb{N}$, let $C_i = C_i(P_0, P_1, \ldots, P_{n-1})$ be the integer defined in Lemma 2.4 associated to a cycle $(P_0, P_1, \ldots, P_{n-1})$. We denote by

$$\mathbb{I}_{i,\mathbb{S}} = \left\{ C_i R_{\mathbb{S}} \,\middle|\, \begin{array}{l} C_i = C_i(P_0, P_1, \ldots, P_{n-1}) \text{ where } (P_0, P_1, \ldots, P_{n-1}) \text{ is a} \\ \text{cycle for a rational map with good reduction outside } S \end{array} \right\} \tag{2.42}$$

and by

$$N(i) = \#(\mathbb{I}_{i,\mathbb{S}}) \tag{2.43}$$

Note that $\mathbb{I}_{i,\mathbb{S}}$ is a set of ideals of $R_{\mathbb{S}}$ but the coefficients C_i are $\mathbb{S}$-integers associated to cycles for rational maps with good reduction outside S. In this definition we use S and not $\mathbb{S}$ because in the proof of Theorem 2.1 we shall use the Morton and Silverman's bound and the Lemma 2.8 which we shall prove after the following:

Lemma 2.7. *With the above notation for every $a, b \in \mathbb{N}$*

$$N(ab) \leq N(a)N(b) \tag{2.44}$$

Proof. We use the same notation of Lemma 2.4.
Let $(P_0, P_1, \ldots, P_{n-1})$ be a cycle for a rational map Φ with good reduction outside S. If $n|a$ or $n|b$ then $C_{ab} = 0$, thus $N(ab) = 1$. Note that $N(i) \geq 1$ for all positive integers i.
Let $n \nmid a$ so that $n \neq 1$ and $(x_0y_1 - x_1y_0)(x_0y_a - x_ay_0) \neq 0$. Let

$$L_{b,a} := \frac{x_0y_{ab} - x_{ab}y_0}{x_0y_a - x_ay_0}\,. \tag{2.45}$$

Since $(P_0, P_a, \ldots, P_{ab}, \ldots)$ is a cycle for the rational map Φ^a which has good reduction outside S and

$$P_{ab} = \underbrace{\Phi^a \circ \ldots \circ \Phi^a}_{b-\text{times}}(P_a),$$

we deduce that the principal ideal

$$L_{b,a}R_{\mathbb{S}} \in \mathbb{I}_{b,\mathbb{S}}. \tag{2.46}$$

Moreover

$$\begin{aligned} C_{ab} &= \frac{x_0y_{ab} - x_{ba}y_0}{x_0y_1 - x_1y_0} && \text{by (2.16) with } i = ab \\ &= \frac{L_{b,a}(x_0y_a - x_ay_0)}{x_0y_1 - x_1y_0} && \text{by (2.45).} \\ &= L_{b,a}C_a && \text{by (2.16) with } i = a. \end{aligned}$$

Now (2.46) and the last identity give (2.7). □

Lemma 2.8. *$N(l) < \infty$ for all positive integers l.*

Proof. We still use the same notation of Lemma 2.4.
We prove this lemma by induction on l. Of course $N(1) = 1$ since $C_1 = 1$. The previous Lemma 2.6 proves the case $l = 2$. Let $l \geq 3$. Now we suppose that Lemma 2.8 holds for every positive integer $< l$. If l is an odd prime number then $l + 1 = 2b$ where b is an integer $1 < b < l$. By Lemma 2.7 $N(2b) \leq N(2)N(b)$, hence by inductive hypothesis $N(l + 1) < \infty$ and $N(l - 1) < \infty$.

Let $(P_0, P_1, \ldots, P_{n-1})$ be a cycle for a rational map with good reduction outside S. By Lemma 2.4-Part 2, the automorphism defined in (2.18) send the ordered n-tupla $(P_0, P_1, \ldots, P_{n-1})$ to the following ordered n-tuple of vectors of K^2

$$(0, 1); (1, 0); \ldots ; (C_l, -C_{l-1}u_{1,l}); (C_{l+1}, -C_l u_{1,l+1}), ; \ldots ; (C_{n-1}, -C_{n-2}u_{1,n-1}) .$$

The identity (2.19) of Lemma 2.4 applied with $i = l$, $j = 1$ tells us that

$$-C_l^2 u_{1,l+1} + C_{l-1}C_{l+1}u_{1,l} = -u_{l,l+1},$$

obtaining an equation like (2.6) of Lemma 2.1

$$C_l^2 = C_{l-1}C_{l+1}\frac{u_{1,l}}{u_{1,l+1}} + \frac{u_{l,l+1}}{u_{1,l+1}} \tag{2.47}$$

By $N(l + 1) < \infty$ and $N(l - 1) < \infty$ we can choose two finite set $\mathscr{C}_{l-1}$, $\mathscr{C}_{l+1}$ such that $C_{l-1}w_1 \in \mathscr{C}_{l-1}$ and $C_{l+1}w_2 \in \mathscr{C}_{l+1}$ for suitable $\mathbb{S}$-units $w_1, w_2 \in R_{\mathbb{S}}^*$. By (2.47), writing

$$C_l^2 = (C_{l-1}w_1C_{l+1}w_2)\frac{u_{1,l}}{u_{1,l+1}w_1w_2} + \frac{u_{l,l+1}}{u_{1,l+1}}$$

we apply Lemma 2.1 with $y = C_l$, $u = u_{1,l}/(u_{1,l+1}w_1w_2)$, $v = u_{l,l+1}/u_{1,l+1}$, $E = 1$ and D one of the $N(l - 1)N(l + 1)$ possible values for $(C_{l-1}w_1C_{l+1}w_2)$. In this way the lemma is proved when l is a prime number.

When l is not a prime number the proof is very easy. Indeed let $l = ab$ where both the integers are $1 < a, b < l$. By inductive hypothesis and Lemma 2.7

$$N(l) \leq N(a)N(b) < \infty$$

□

Now we are ready to prove Theorem 2.1

Proof of Theorem 2.1. Let $(P_0, P_1, \dots, P_{n-1})$ be a cycle for a rational map Φ with good reduction outside S. Of course for every set $\mathbb{S}$, of places of K, which contains S, the rational map Φ has good reduction outside $\mathbb{S}$. For a generic fixed $\mathbb{S}$ such that $R_{\mathbb{S}}$ is a P.I.D. we denote by

$$\mathfrak{I}_{i,\mathbb{S}} = \prod_{\mathfrak{p} \notin \mathbb{S}} \mathfrak{p}^{\delta_{\mathfrak{p}}(P_0,P_i)}$$

for all indexes $1 \leq i \leq (n-1)$. It follows that

$$\mathfrak{I}_{i,\mathbb{S}}\mathfrak{I}_{1,\mathbb{S}}^{-1} = \left(\frac{x_0y_i - x_iy_0}{x_0y_1 - x_1y_0}\right)R_{\mathbb{S}}.$$

We have used the usual notation $P_j = [x_j : y_j]$ where x_j, y_j are coprime $\mathbb{S}$-integers for all points P_j of the cycle. By (2.16) of Lemma 2.4-Part 1 it is clear that $\mathfrak{I}_{i,\mathbb{S}}\mathfrak{I}_{1,\mathbb{S}}^{-1} \in \mathbb{I}_{i,\mathbb{S}}$.

Now we use the bound found by Morton and Silverman (see Proposition 1.4 and Theorem 1.4) from which it follows that n (the minimal period of P_0) is smaller than

$$[12(s+1)\log(5(s+1))]^{8s}. \tag{2.48}$$

To ease notation, we denote by B this bound. The existence of this bound B tells us that, for every index $j > B$, $\mathbb{I}_{j,\mathbb{S}}$ is the empty set. Therefore we take

$$\mathbb{I}_{\mathbb{S}} = \bigcup_{1 \leq i \leq B} \mathbb{I}_{i,\mathbb{S}}.$$

By Lemma 2.8 the set $\mathbb{I}_{\mathbb{S}}$ is a finite union of finite sets, thus it is finite. By Lemma 2.4

$$\mathfrak{I}_{i,\mathbb{S}}\mathfrak{I}_{1,\mathbb{S}}^{-1} = C_iR_{\mathbb{S}} \in \mathbb{I}_{\mathbb{S}}.$$

In other words, let $\mathfrak{I}_i$ be the ideal of R_S defined in (2.14) associated to a cycle. We have proved that there exist a finite set $T_{\mathbb{S}}$ of prime ideals, such that $T_{\mathbb{S}} \cap \mathbb{S} = \emptyset$, and a constant $C_{\mathbb{S}}$ such that: for every cycle $(P_0, P_1, \dots, P_{n-1})$ for rational maps with good reduction outside S and for every index $1 \leq i \leq (n-1)$,

$$\mathfrak{I}_i\mathfrak{I}_1^{-1} = \prod_{\mathfrak{p} \in \mathbb{S} \setminus S} \mathfrak{p}^{e_{\mathfrak{p}}} \prod_{\mathfrak{p} \in T_{\mathbb{S}}} \mathfrak{p}^{e_{\mathfrak{p}}} \tag{2.49}$$

where for all $\mathfrak{p} \in T_{\mathbb{S}}$ the exponent $0 \leq e_{\mathfrak{p}} \leq C_{\mathbb{S}}$. Note that at this point we are not in the position to state that also the exponents of the prime ideals in $\mathbb{S} \setminus S$ are

positive and bounded from above by an uniform constant which does not depend on the cycle.
If R_S is a P.I.D. we have finished. Indeed from $\mathbb{S} = S$ the proof is finished by taking $\mathbb{I}_S = \mathbb{I}_{\mathbb{S}}$.

If R_S is not a P.I.D., then there exist two disjoint finite sets S_1, S_2 of prime ideals, of cardinality equal to the class number of R_S minus 1, such that $R_{S\cup S_1}$ and $R_{S\cup S_2}$ are P.I.D.. This follows immediately from "Dirichlet's Theorem"about the uniform distribution of the prime ideals among the ideal classes [20, Chapter 8]. We denote by $\mathbb{S}_1 = S \cup S_1$ and $\mathbb{S}_2 = S \cup S_2$. For each $k \in \{1, 2\}$ we repeat the previous reasoning did with $\mathbb{S}$. In this way we prove that there exist a finite set $T_{\mathbb{S}_k}$ and a constant $C_{\mathbb{S}_k}$ such that $T_{\mathbb{S}_k} \cap \mathbb{S}_k = \emptyset$ and

$$\mathfrak{I}_i\mathfrak{I}_1^{-1} = \prod_{\mathfrak{p}\in\mathbb{S}_k\setminus S} \mathfrak{p}^{e_\mathfrak{p}} \prod_{\mathfrak{p}\in T_{\mathbb{S}_k}} \mathfrak{p}^{e_\mathfrak{p}}$$

with $0 \leq e_\mathfrak{p} \leq C_{\mathbb{S}_k}$ for all $\mathfrak{p} \in T_{\mathbb{S}_k}$. From $(\mathbb{S}_1 \setminus S) \cap (\mathbb{S}_2 \setminus S) = \emptyset$ it follows that

$$\mathfrak{I}_i\mathfrak{I}_1^{-1} = \prod_{\mathfrak{p}\in T_{\mathbb{S}_1}\cup T_{\mathbb{S}_2}} \mathfrak{p}^{e_\mathfrak{p}}$$

with $0 \leq e_\mathfrak{p} \leq \max\{C_{\mathbb{S}_1}, C_{\mathbb{S}_2}\}$. Therefore theorem holds by taking

$$\mathbb{I}_S = \left\{ \prod_{\mathfrak{p}\in T_{\mathbb{S}_1}\cup T_{\mathbb{S}_2}} \mathfrak{p}^{e_\mathfrak{p}} \mid 0 \leq e_\mathfrak{p} \leq \max\{C_{\mathbb{S}_1}, C_{\mathbb{S}_2}\} \right\}. \tag{2.50}$$

□

The proof of Theorem 2.1 contained in [6] is a little different from the proof presented in this thesis. Recall that the cross-ratio of four distinct points P_1, P_2, P_3, P_4 of $\mathbb{P}_1(K)$ is

$$\varrho(P_1, P_2, P_3, P_4) = \frac{(x_1y_3 - x_3y_1)(x_2y_4 - x_4y_2)}{(x_1y_2 - x_2y_1)(x_3y_4 - x_4y_3)}.$$

Morton and Silverman used cross-ratio to produce S-units from cycles for rational maps with good reduction outside S. Instead, in the proof in [6], we used the following property

$$\varrho(P_1, P_2, P_3, P_4) + \varrho(P_1, P_2, P_4, P_3) = 1,$$

to produce S-unit equations.

Proof of Corollary 2.1. Let $C_{\mathbb{S}_1}, C_{\mathbb{S}_2}$ be the integers and $T_{\mathbb{S}_1} \cup T_{\mathbb{S}_2}$ be the set of places defined in the previous proof. Fixing two consecutive points $P_0, P_1 \in \mathbb{P}_1(K)$ of a cycle $(P_0, P_1, \dots, P_{n-1})$ we set the ideal $\mathfrak{I}_1$ defined by (2.14). By Theorem 2.1 it results that

$$0 \leq \delta_{\mathfrak{p}}(P_0, P_k) \leq \delta_{\mathfrak{p}}(P_0, P_1) + \max\{C_{\mathbb{S}_1}, C_{\mathbb{S}_2}\}$$

for all indexes $1 \leq k \leq (n-1)$ and in particular $\delta_{\mathfrak{p}}(P_0, P_k) = \delta_{\mathfrak{p}}(P_0, P_1)$ for all prime ideals $\mathfrak{p} \notin T_{\mathbb{S}_1} \cup T_{\mathbb{S}_2}$. Thus, by Proposition 2.2-Part (a) it follows that for every distinct points P_i, P_j of the cycle

$$\delta_{\mathfrak{p}}(P_i, P_j) = \delta_{\mathfrak{p}}(P_0, P_1) \quad \text{for all } \mathfrak{p} \notin T_{\mathbb{S}_1} \cup T_{\mathbb{S}_2}$$

and

$$\delta_{\mathfrak{p}}(P_i, P_j) \leq \delta_{\mathfrak{p}}(P_0, P_1) + \max\{C_{\mathbb{S}_1}, C_{\mathbb{S}_2}\} \quad \text{for all } \mathfrak{p} \in T_{\mathbb{S}_1} \cup T_{\mathbb{S}_2}.$$

Note that, for all but finitely many prime ideals $\mathfrak{p}$, $\delta_{\mathfrak{p}}(P_0, P_1) = 0$.
Now applying the results of Birch and Merriman [5], with the same method used in the proof of Proposition 1.2, we prove the first part of this corollary. For the proof of the second part see the following Remark 2.1. □

Proof of Corollary 2.2. Let $(P_0, P_1, \dots, P_{n-1})$ be a cycle for a rational map with good reduction outside S. We still work with the enlarged set $\mathbb{S}$. We still use the notation $P_i = [x_i : y_i]$, where x_i, y_i are coprime $\mathbb{S}$-integers, for all points of the cycle. By Theorem 2.1 we can choose a finite set of non zero $\mathbb{S}$-integers $\mathscr{C}_{\mathbb{S}}$, which does not depend on the particular choice of the cycle, such that for every $1 \leq i \leq (n-1)$

$$\left(\frac{x_0 y_i - x_i y_0}{x_0 y_1 - x_1 y_0}\right) R_{\mathbb{S}} = C_i R_{\mathbb{S}}$$

for a suitable $\mathbb{S}$-integer $C_i \in \mathscr{C}_{\mathbb{S}}$. The automorphism of $\mathbb{P}_1(K)$, associated to the matrix A defined in (2.18), maps the cycle $(P_0, P_1, \dots, P_{n-1})$ to the following ordered n-tuple of points in $\mathbb{P}_1(K)$

$$([0:1], [1:0], [C_2 : u_2], \dots, [C_i : u_i], \dots, [1 : u_{n-1}]) \tag{2.51}$$

where for each $2 \leq i \leq (n-1)$, u_i is a suitable $\mathbb{S}$-unit and $C_i \in \mathscr{C}_{\mathbb{S}}$. The automorphism associated to the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & u_2^{-1} \end{pmatrix} \in \mathrm{PGL}_2(R_{\mathbb{S}})$$

maps the previous n-tuple to the following:

$$([0:1],[1:0],[C_2:1],\dots,[C_i:v_i],\dots,[1:v_{n-1}]) \tag{2.52}$$

where the v_i's still are $\mathbb{S}$-units.
Of course, since the last n-tuple is obtained from (2.51) by action of an element of $\mathrm{PGL}_2(R_{\mathbb{S}})$, the equations type (2.19) still holds. In particular for every index $3 \le i \le (n-1)$, there exists a $\mathbb{S}$-unit w_i such that

$$C_2v_i - C_i = C_{i-2}w_i$$

Now it is clear that we can choose

$$\mathcal{N} = \left\{ n\text{-tuples like (2.52)} \;\middle|\; \begin{array}{l} n \le B, \text{ for all indexes } i, C_i \in \mathscr{C}_{\mathbb{S}} \text{ and there} \\ \text{exists } w \in R_{\mathbb{S}}^* \text{ such that } (v_i, w) \text{ is a solution} \\ \text{of } Cv_i - D = Ew \text{ with } C, D, E \in \mathscr{C}_{\mathbb{S}} \end{array} \right\}$$

where B is the bound (2.48). By the finiteness of the set $\mathscr{C}_{\mathbb{S}}$ and the $\mathbb{S}$ unit equation Theorem applied to the finitely many equations $Cv_i - D = Ew$ it results that $\mathcal{N}$ is a finite set. □

Remark 2.1. From the previous proof it results that for every couple $\{P_0, P_1\}$ of points in $\mathbb{P}_1(K)$, *the set of inequivalent cycles that contain two fixed points P_0 and P_1 as consecutive points* has cardinality bounded by $|\mathcal{N}|$. With the same arguments used in this chapter, more generally it is easy to see that to obtain uniform finiteness it is sufficient to require that the points P_0, P_1 are elements of a cycle in arbitrary position.

2.4 An unboundedness result

Theorem 2.2. *Let $K = \mathbb{Q}$ and $S = \{|\cdot|_\infty; |\cdot|_2\}$. There exist infinitely many ideals $\mathfrak{I}$ for which there exists a 3-cycle (P_0, P_1, P_2), for a suitable rational map of degree 4 with good reduction outside S, for which $\mathfrak{I}_1 = \mathfrak{I}$ holds, where $\mathfrak{I}_1$ is the ideal defined in (2.14).*

Theorem 2.2 proves that the conclusion of Theorem 2.1 is in a sense best-possible: for every cycle one has

$$(\mathfrak{I}_1, \dots, \mathfrak{I}_{n-1}) = \mathfrak{I}_1(R_S, \mathfrak{I}_2\mathfrak{I}_1^{-1}, \dots, \mathfrak{I}_{n-1}\mathfrak{I}_1^{-1})$$

where for the factor $(R_S, \mathfrak{I}_2\mathfrak{I}_1^{-1}, \dots, \mathfrak{I}_{n-1}\mathfrak{I}_1^{-1})$ there are only finitely many possibilities in view of Theorem 2.1, but not for the factor $\mathfrak{I}_1$, in view of Theorem 2.2.

Proof of Theorem 2.2. Let

$$\mathcal{T} := \{([u : u-1], [u-1 : -1], [1 : u]) \mid u \in R_S^*\}.$$

We take U the automorphism of $\mathbb{P}_1(\mathbb{Q})$ associated to the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in \mathrm{PGL}_2(\mathbb{Z}).$$

The automorphism U has order 3 in $\mathrm{PGL}_2(\mathbb{Z})$ and more precisely, for all $u \in R_S^*$

$$U([u : u-1]) = [u-1 : -1]\ ,\ U([u-1 : -1]) = [1 : u]\ ,\ U([1 : u]) = [u : u-1].$$

Thus every element of $\mathcal{T}$ is a cycle for U.
In this proof, for every $u \in R_S^*$ we will show that

$$([u : u-1], [u-1 : -1], [1 : u])$$

is a cycle for a rational map Φ_u of degree 4 with good reduction outside S.

To simplify the notation, to each rational map $\phi\colon \mathbb{P}_1 \to \mathbb{P}_1$ defined over $\mathbb{Q}$ we shall associate, in the canonical way, the rational function $\phi(z) \in \mathbb{Q}(z)$ by taking the pole of z as the point at infinity $[1 : 0]$. Writing a rational function $\phi(z) = N(z)/D(z)$ it will mean that $N, D \in \mathbb{Z}[z]$ are coprime polynomials. In this way a rational function ϕ will have good reduction at a prime p if and only if p does not divide the resultant of polynomials F, D and furthermore if $\tilde{\phi}$, the rational function obtained from ϕ by reduction modulo p, has the same degree of ϕ. Writing $\mathbb{P}_1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, we will shift from the homogeneous to the affine notation for points in $\mathbb{P}_1(\mathbb{Q})$ when necessary. So that the point $[1 : 0]$ will correspond to ∞ and any other point $[x : y]$ will correspond to the rational number x/y.
By this notation the automorphism U becomes $U(z) = (1-z)^{-1}$ and for every $x/y \in \mathbb{Q}$ it follows that

$$U\left(\frac{x}{y}\right) = \frac{y}{y-x};\ \ U^2\left(\frac{x}{y}\right) = \frac{y-x}{-x} \ \text{ and } \ U^3\left(\frac{x}{y}\right) = \frac{x}{y}.$$

The starting point to define the rational maps Φ_u is to see that U admits the following cycles:

$$0 \mapsto 1 \mapsto \infty \mapsto 0; \quad -1 \mapsto \frac{1}{2} \mapsto 2 \mapsto -1.$$

Therefore the degree three function $\psi(z) \in \mathbb{Q}(z)$ defined by

$$\psi(z) = \frac{(z+1)(2z-1)(z-2)}{2z(z-1)}$$

has exactly the same zeroes and poles of the function $\psi \circ U$, thus there exists a constant λ such that $\psi = \lambda(\psi \circ U)$. It is an easy computation to see that this constant is equal to 1 obtaining

$$\psi = \psi \circ U. \tag{2.53}$$

Moreover it is another simple computation to see that ψ has good reduction outside S.

Let u be a fixed S-integer. Let us define $P_0 = u/(u-1)$, $P_1 = U(u/(u-1)) = -(u-1)$ and $P_2 = U^2(u/(u-1)) = 1/u$ so that $(P_0, P_1, P_2) \in \mathcal{T}$. Since

$$\psi(P_0) = \frac{-2u^3 + 3u^2 + 3u - 2}{2u^2 - 2u}$$

the degree one rational function

$$h_u(z) = \frac{(4u^2 - 4u)z - (-4u^3 + 6u^2 + 6u - 4)}{2uz + 4u^2 + u - 2}$$

verifies $h_u(\psi(P_0)) = 0$ and it has good reduction outside S since u is a S-unit. Now we take the rational function

$$h_u \circ \psi(z) = \frac{(2u^2 - 2u)z^3 + (2u^3 - 6u^2 + 2)z^2 + (-2u^3 + 6u - 2)z + (2u^2 - 2u)}{uz^3 + (2u^2 - u - 1)z^2 + (-2u^2 - 2u + 1)z + u}.$$

By definition of the map h_u and by (2.53) it results

$$h_u \circ \psi(P_0) = h_u \circ \psi(P_1) = h_u \circ \psi(P_2) = 0. \tag{2.54}$$

Of course the rational function $h_u \circ \psi$ has good reduction outside S. Let us define $\psi_u(z) = z + h_u \circ \psi(z)$. Now we prove a lemma useful to prove that the map ψ_u has good reduction outside S.

Lemma 2.9. *Let $\phi \in \mathbb{Q}(z)$ be a rational map with good reduction outside S such that $\phi(\infty) = \infty$, let $\begin{pmatrix} a & b \\ u & c \end{pmatrix} \in \mathrm{GL}_2(R_S)$ and put*

$$t(z) = \frac{az + b}{uz + c}.$$

Then the rational function $z + t \circ \phi(z)$ has degree $\deg(\phi) + 1$ *and has good reduction outside S if and only if $u \in R_S^*$.*

Proof. Let $\phi(z) = N(z)/D(z)$ where $N, D \in \mathbb{Z}[z]$ are polynomials with no common factors. Since $\phi(\infty) = \infty$ we have that $\deg(\phi) = \deg(N) > \deg(D)$ and since ϕ has good reduction outside S one has that the leading coefficient of N is a S-unit and N, D have no common factors modulo any prime $p \notin S$. It is clear that also the rational function

$$t \circ \phi(z) = \frac{aN(z) + bD(z)}{uN(z) + cD(z)}$$

has good reduction outside S. Thus the polynomials $(aN(z) + bD(z))$,$(uN(z) + cD(z))$ have no common factors modulo any prime $p \notin S$ and have the same degree of ϕ. Moreover the leading coefficient of $(uN(z) + cD(z))$ is a S-unit if and only if $u \in R_S^*$. Now it is immediate to see that the rational function

$$z + t \circ \phi(z) = \frac{(uN(z) + cD(z))z + (aN(z) + bD(z))}{(uN(z) + cD(z))}$$

has degree equal to $\deg(\phi) + 1$ and has good reduction outside S if and only if $u \in R_S^*$. □

Since $\psi(\infty) = \infty$, we can apply Lemma 2.9 with $\phi = \psi$ and $t = h_u$ so that ψ_u has good reduction outside S since $u \in R_S^*$. Moreover ψ_u has degree equal to 4 and by (2.54) it follows that

$$\psi_u(P_i) = P_i \text{ for every index } i \in \{0, 1, 2\}. \tag{2.55}$$

Finally we can define

$$\phi_u = U \circ \psi_u.$$

Let Φ_u be the endomorphism of $\mathbb{P}_1$ given by ϕ_u. Of course Φ_u has degree 4 and good reduction outside S. By (2.55) the 3-tuple (P_0, P_1, P_2) is a cycle for Φ_u.
In this way we have proved that for all $u \in R_S^*$, more precisely for every n-th power of 2, the 3-tuple

$$([2^n : 2^n - 1]; [2^n - 1 : -1]; [1 : 2^n]) \in \mathcal{T}$$

is a cycle for a rational map of degree 4 with good reduction outside S and $\Im_1 = \Im_2 = (2^{2n} - 2^n + 1) \cdot \mathbb{Z}[1/2]$. Note that the set of prime divisors of $(2^{2n} - 2^n + 1)$ for $n \in \mathbb{N}$ is infinite. This concludes the proof of Theorem 2.2. □

Actually, we have proved Theorem 2.2 for every number field K and every choice of finite set S containing all archimedean places of K and the 2-adic ones. Moreover, to prove Theorem 2.2 we have used an automorphism $U \in \mathrm{PGL}_2(\mathbb{Z})$ of order 3. For any positive integer n, with a suitable number field K and a suitable finite set S of places, by using an automorphism of $\mathrm{PGL}_2(R_S)$ of order n, it is possible to employ the same method used in the proof of Theorem 2.2. Probably in this way it is possible to define an infinite set of n-cycles which satisfy Theorem 2.2.

Chapter 3

Finite rational orbits for rational maps

3.1 Introduction

In this chapter we shall prove two new results about finite orbits for rational maps with good reduction outside S. The first is the following:

Theorem 3.1. *Let K be a number field and let R be ring of algebraic integers of K. Let S be a finite set of places of K, with cardinality s, containing all the archimedean ones. There exists a number $c(s, h_S)$, depending only on s and the class number h_S of R_S, such that the length of every finite orbit in $\mathbb{P}_1(K)$, for rational maps with good reduction outside S, is bounded by $c(s, h_S)$. We can choose $c(s, h_S)$ equal to*

$$2^{1045(s+h_S-1)} \left[12(s+1)\log(5s+5)\right]^{8s}. \tag{3.1}$$

For particular fields and particular sorts of maps the bound (3.1) may be greatly improved. For example, in the elementary case with $K = \mathbb{Q}$. It is easy to see that every polynomial in $\mathbb{Z}[x]$ has cycles in $\mathbb{Z}$ of length at most 2. Narkiewicz and Pezda in [25] proved that every finite orbit in $\mathbb{Z}$ has cardinality at most 4. Another elementary example is the case of finite orbits for element of $\mathrm{PGL}_2(R_S)$ in which the bound can be chosen $c(s, h_S) = 2 + 16s^2$ (see Proposition 1.35).

Recently R. Benedetto has obtained a bound for polynomial maps. He proved in [3] that if $\phi \in K[z]$ is a polynomial of degree $d \geq 2$ which has bad reduction at s prime ideals of K, then the number of preperiodic points of ϕ is at most $O(s \log s)$. The big-O constant is essentially $(d^2 - 2d + 2)/\log d$ for large s (see [3, Theorem

7.1]. Benedetto's proof relies on a detailed analysis of $\mathfrak{p}$-adic Julia sets. Actually, Benedetto's result is quite different from Theorem 3.1. In fact Benedetto's result concern only polynomial map and its bound also depends on the degree d of a polynomial. But it is a very strong result because it limits the cardinality of the whole set of preperiodic points. Furthermore, in terms of s, Benedetto's bound is better than (3.1).

Recall that in all part of this thesis we use the notation set at the beginning of section §1.2.

we shall end this chapter by giving the proofs of two theorems which are a sort of generalization to finite orbits of the Corollary 2.1.

Theorem 3.2. *Let $n \geq 4$. The set of orbits in $\mathbb{P}_1(K)$ for rational maps with good reduction outside S which contain a given n-cycle is finite.*
Let $n \in \{2, 3\}$. Given a cycle $(P_0, \ldots, P_{n-1})$ and a point P_{-1} in $\mathbb{P}_1(K)$ there are only finitely many orbits in $\mathbb{P}_1(K)$ for rational maps with good reduction outside S of the form $(P_{-m}, \ldots, P_{-1}, P_0, \ldots, P_{n-1})$.

If K has class number one, then this last result is effective since the finiteness follows from the S-unit equation Theorem in two variables. But the proof obtained depends on the choice of the cycle.

Corollary 2.1 states that there are only finitely many cycle classes, for rational maps with good reduction outside S, which contain two fixed consecutive points. Thus in the hypothesis of Theorem 3.2, to obtain finiteness for the cycle classes, it is sufficient to fix only two consecutive points of a cycle. But the proof of Corollary 2.1 is not effective.

The case $n = 1$ is quite different from the other ones. Indeed given a fixed point P_0 and another point P_{-1}, there could exist infinitely many orbits of the form $(P_{-m}, \ldots, P_{-1}, P_0)$. Recall that two ordered n-tuples are called equivalent if they belong to the same orbit for the action of $\mathrm{PGL}_2(R_S)$ on n-tuples.

Theorem 3.3. *Given two distinct points $P_0, P_{-1} \in \mathbb{P}_1(K)$, there exist only finitely many inequivalent orbits in $\mathbb{P}_1(K)$, of the form $(P_{-m}, \ldots, P_{-1}, P_0)$, for a rational map Φ with good reduction outside S such that $\Phi(P_0) = P_0$.*

This last result is a direct consequence of Birch-Merriman's Theorem [5] about the finiteness of binary forms with given degree and discriminant. Also in this case if K has class number one, then using the effective result obtained by J. H. Evertse and K.Győry [10], the Theorem 3.3 is effective but the finiteness result depends on the choice of the points $P_0, P_{-1} \in \mathbb{P}_1(K)$.

3.2 Finite orbit lengths for rational maps

This section is dedicated to prove Theorem 3.1.

If R_S is not a P.I.D. we still take the enlarged set $\mathbb{S}$ (the set defined at the beginning of §2.3) so that $R_{\mathbb{S}}$ is a unique factorization domain. In this chapter we still use the convention that the ordered couple (x_i, y_i) always represents coprime $\mathbb{S}$-integral homogeneous coordinates for every point $P_i \in \mathbb{P}_1(K)$. In this chapter we study finite orbits. From this we cannot use Proposition 2.2, since in a finite orbit there can exist some preperiodic points which are not periodic and for these points the identity stated in Proposition 2.2 could not be held. But the congruence properties expressed in Proposition 2.1 and Proposition 2.3 hold also in this situation.

Writing $(Q_{-k}, \dots, Q_0, \dots, Q_{n-1})$ we represent a finite orbit for a rational map Ψ in which the 0-th term Q_0 is a n-th periodic point for Ψ. Moreover, for all indexes $i \geq -k$, $Q_{i+1} = \Psi(Q_i)$ holds, bearing in mind that $Q_n = Q_0$. Now we present a very simple remark which will be useful in the sequel.

Remark 3.1. *Let $(Q_{-k}, \dots, Q_0, \dots, Q_{n-1})$ be a finite orbit in $\mathbb{P}_1(K)$ for a rational map Ψ with good reduction outside S; then for all integers $-k \leq a \leq n-1, b \geq 0, t \geq 0$ and for every prime ideal $\mathfrak{p} \notin S$*

$$\begin{aligned}&\delta_{\mathfrak{p}}(Q_a, Q_{a+tb}) \geq \\ &\qquad \min\{\delta_{\mathfrak{p}}(Q_a, Q_{a+b}), \delta_{\mathfrak{p}}(Q_{a+b}, Q_{a+2b}), \dots, \delta_{\mathfrak{p}}(Q_{a+(t-1)b}, Q_{a+tb})\} = \delta_{\mathfrak{p}}(Q_a, Q_{a+b})\end{aligned}$$

Proof. It is a direct application of the triangle inequality (Proposition 2.1) and Proposition 2.3. In fact the b-th iterate of Ψ still has good reduction at every prime ideal $\mathfrak{p} \notin S$, therefore

$$\delta_{\mathfrak{p}}(Q_{a+lb}, Q_{a+(l+1)b}) = \delta_{\mathfrak{p}}(\Psi^b(Q_{a+(l-1)b}), \Psi^b(Q_{a+lb})) \geq \delta_{\mathfrak{p}}(Q_{a+(l-1)b}, Q_{a+lb})$$

for all indexes $0 < l \leq t$. □

We begin the proof of Theorem 3.1 by reducing to the case when the tuple $(P_{-m}, \dots, P_{-1}, P_0)$ is an orbit for a rational map Φ with good reduction outside $\mathbb{S}$ and $P_0 = [0 : 1]$ is a fixed point of Φ. Let $(Q_{-k}, \dots, Q_{-1}, Q_0, \dots, Q_{n-1})$ be a finite orbit for a endomorphism Ψ on $\mathbb{P}_1$ defined over K with good reduction outside $\mathbb{S}$ and let $(Q_0, \dots, Q_{n-1})$ a cycle for Ψ. If $k \leq n$ we have nothing to prove since n is bounded by (1.36) so that the finite orbit has cardinality limited by two times the bound (1.36). Suppose now that $k > n$; it is clear that the

tuple $\left(Q_{-\lfloor\frac{k}{n}\rfloor n},\ldots,Q_{-n},Q_O\right)$ is an orbit for Ψ^n and Q_0 is a fixed point. Take an automorphism $A\in\mathrm{PGL}_2(R_{\mathbb{S}})$ such that $A(Q_0)=[0:1]$, of course there exists since $R_{\mathbb{S}}$ is a P.I.D., then $\left(A(Q_{-\lfloor\frac{k}{n}\rfloor n}),\ldots,A(Q_{-n}),[0:1]\right)$ is an orbit for $A\Psi^nA^{-1}$, which still has good reduction outside S. Therefore we take $P_{-m}=A\left(Q_{-\lfloor\frac{k}{n}\rfloor n}\right)$ and for all indexes $\left\lfloor\frac{k}{n}\right\rfloor=m\geq i\geq 0$, $P_{-m+i}=(A\Psi^nA^{-1})^i(P_{-m})$. In this way if we find a bound b for the cardinality of orbits of type $(P_{-m},\ldots,P_{-1},P_0)$, where P_0 is a fixed point, then the bound $c(s,h_S)$ can be chosen equal to $(b+1)$ multiplied by the upper bound for the cycle length provided by (1.36).
Now let us search for such a bound b. Let

$$(P_{-m},\ldots,P_{-1},P_0)\tag{3.2}$$

be a finite orbit in $\mathbb{P}_1(K)$ for a rational map Φ with good reduction outside $\mathbb{S}$ and such that $\Phi(P_0)=P_0=[0:1]$.

Lemma 3.1. *Let $P_{l-k},\ldots,P_{l-1},P_l$ be distinct points of the orbit (3.2) such that for every prime ideal $\mathfrak{p}\notin\mathbb{S}$*

$$\delta_{\mathfrak{p}}(P_{l-i},P_0)=\delta_{\mathfrak{p}}(P_l,P_0)\ \text{for every index } 0\leq i\leq k.\tag{3.3}$$

Then

$$k\leq 3\cdot 7^{|\mathbb{S}|}+1.\tag{3.4}$$

Proof. Recall that by convention for every index j the ordered couple (x_j,y_j) denotes coprime $\mathbb{S}$-integral homogeneous coordinates for the point P_j. Since $P_0=[0:1]$, condition (3.3) is equivalent to the following identities between principal ideals

$$x_{l-i}R_{\mathbb{S}}=x_lR_{\mathbb{S}}\ \text{ for all indexes } 0\leq i\leq k.$$

Hence condition (3.3) is equivalent to the existence, for each index $0\leq i\leq k$, of a $\mathbb{S}$-unit u_{l-i} such that

$$x_{l-i}=x_lu_{l-i}.\tag{3.5}$$

From this, it follows that for every prime ideal $\mathfrak{p}\notin\mathbb{S}$ and for all indexes $k\geq i>j\geq 0$

$$\begin{array}{rcll}\delta_{\mathfrak{p}}(P_{l-i},P_{l-j}) & = & v_{\mathfrak{p}}(x_{l-i}y_{l-j}-x_{l-j}y_{l-i}) & \text{by choice of } S\text{-coprime coordinates}\\ & \geq & v_{\mathfrak{p}}(x_l) & \text{by (3.5)}\\ & = & \delta_{\mathfrak{p}}(P_l,P_0) & \text{since } P_0=[0:1].\end{array}\tag{3.6}$$

Moreover we can apply Remark 3.1 to the orbit $(P_{-m},\dots,P_{-1},P_0)$ with $a = l - i$, $b = i - j$ and t such that $l - i + t(i - j) \geq 0$, obtaining that

$$\begin{aligned} \delta_{\mathfrak{p}}(P_{l-i},P_0) &\geq \min\{\delta_{\mathfrak{p}}(P_{l-i},P_{l-j}),\delta_{\mathfrak{p}}(P_{l-j},P_{l+i-2j}),\dots,\delta_{\mathfrak{p}}(P_{l-i+(t-1)(i-j)},P_0)\} \\ &= \delta_{\mathfrak{p}}(P_{l-i},P_{l-j}). \end{aligned} \tag{3.7}$$

Thus

$$\begin{aligned} \delta_{\mathfrak{p}}(P_l,P_0) &\leq \delta_{\mathfrak{p}}(P_{l-i},P_{l-j}) && \text{by (3.6)} \\ &\leq \delta_{\mathfrak{p}}(P_{l-i},P_0) && \text{by (3.7)} \\ &= \delta_{\mathfrak{p}}(P_l,P_0) && \text{by (3.3),} \end{aligned}$$

which tells us

$$\delta_{\mathfrak{p}}(P_l,P_0) = \delta_{\mathfrak{p}}(P_{l-i},P_{l-j}). \tag{3.8}$$

Furthermore by (3.5), for every index $i \in \{0,\dots,k\}$, we can write $P_{l-i} = [x_l : y_{l-i}/u_{l-i}]$ in homogeneous coprime $\mathbb{S}$-integral coordinates; hence from (3.8) it follows that

$$v_{\mathfrak{p}}(x_0y_l - x_ly_0) = v_{\mathfrak{p}}\left(\frac{x_ly_{l-j}}{u_{l-j}} - \frac{x_ly_{l-i}}{u_{l-i}}\right).$$

Since $P_0 = [0 : 1]$, the above identity is equivalent to the existence of a $\mathbb{S}$-unit $u_{l-i,l-j}$ such that

$$\frac{y_{l-j}}{u_{l-j}} - \frac{y_{l-i}}{u_{l-i}} = u_{l-i,l-j} \in R_{\mathbb{S}}^{*} \tag{3.9}$$

for all distinct indexes $i, j \in \{0,\dots,k\}$. In particular, either $k \in \{0,1\}$ or we have a system of three equations

$$\begin{cases} y_l - y_{l-1}/u_{l-1} = u_{l-1,l} \\ y_l - y_{l-i}/u_{l-i} = u_{l-i,l} \\ y_{l-1}/u_{l-1} - y_{l-i}/u_{l-i} = u_{l-i,l-1}. \end{cases} \tag{3.10}$$

The first one is obtained from (3.9) substituting $j = 0$ and $i = 1$ (recall that $u_l = 1$) and the two other ones with $j = 0$, $j = 1$ and i an arbitrary index $k \geq i \geq 2$.
We deduce from (3.10) the following linear relation:

$$u_{l-1,l} + u_{l-i,l-1} = u_{l-i,l}.$$

By the $\mathbb{S}$-unit equation Theorem, for every index $k \geq i \geq 2$, there are only finitely many possibilities for $u_{l-i,l}/u_{l-1,l}$ and from (3.10) it follows that

$$\frac{y_{l-i}}{u_{l-i}} = y_l - \frac{u_{l-i,l}}{u_{l-1,l}}u_{l-1,l}.$$

By Evertse's result [8], the number of $\mathbb{S}$-unit solutions $(u, v) \in R_{\mathbb{S}}^* \times R_{\mathbb{S}}^*$ to the equation $u + v = 1$ is at most $3 \cdot 7^{4|\mathbb{S}|}$.
Hence the set of points $\{P_{l-i} = [x_l : y_{l-i}/u_{l-i}] \mid k \geq i \geq 2\}$ has cardinality bounded by $3 \cdot 7^{4|\mathbb{S}|}$ so that $k \leq (3 \cdot 7^{4|\mathbb{S}|} + 1)$. □

The next step is to show that the number of points P_{-i} of (3.2) such that $x_{-i}R_{\mathbb{S}} \neq x_{-i+1}R_{\mathbb{S}}$ is finite and depends only on $|\mathbb{S}|$. We have to prove two lemmas.

We say that a non zero $\mathbb{S}$-integer T is representable in *two essentially different ways* as sum of two $\mathbb{S}$-units if there exist

$$u_1, u_2, v_1, v_2 \in R_{\mathbb{S}}^*, \{u_1, u_2\} \neq \{v_1, v_2\} \text{ and } T = u_1 + u_2 = v_1 + v_2 \neq 0. \tag{3.11}$$

Lemma 3.2. *The cardinality of the set of principal ideals of* $R_{\mathbb{S}}$

$$\{T \cdot R_{\mathbb{S}} \mid T \textit{ satisfies (3.11)}\}$$

is bounded by $2^{1031 \cdot |\mathbb{S}|}$.

Proof. Let $T \in R_{\mathbb{S}}/\{0\}$ be written as $T = u_1 + u_2 = v_1 + v_2$ which satisfies the condition in (3.11). Therefore, since $\{u_1, u_2\} \neq \{v_1, v_2\}$, the left term of equation

$$\frac{u_1}{v_1} + \frac{u_2}{v_1} - \frac{v_2}{v_1} = 1$$

has no vanishing subsums. Using the Evertse's bound [11] for the number of non degenerated solutions $(w_1, w_2, w_3) \in (R_{\mathbb{S}}^*)^3$ to the equation $X_1 + X_2 + X_3 = 1$, we obtain that the principal ideal

$$T \cdot R_{\mathbb{S}} = v_1 \left(1 + \frac{v_2}{v_1}\right) \cdot R_{\mathbb{S}}$$

has at most $2^{1031 \cdot |\mathbb{S}|}$ possibilities. □

This result is an elementary application of $\mathbb{S}$-unit equation Theorem in three variables. Halter-Koch and Narkiewicz stated this fact in [14] but we have presented this lemma because we need a quantitative result.

Remark 3.2. The previous lemma states that the set of principal ideals of $R_{\mathbb{S}}$ generated by an non zero $\mathbb{S}$-integer which is representable, in two essentially different ways, as sum of two $\mathbb{S}$-units, has cardinality bounded by $2^{1031 \cdot |\mathbb{S}|}$. Thus we can choose a set $\mathfrak{T}$ of $\mathbb{S}$-integers, with cardinality at most $2^{1031 \cdot |\mathbb{S}|}$, such that every $\mathbb{S}$-integer with the property (3.11) is representable as uT, where $u \in R_{\mathbb{S}}^*$ and $T \in \mathfrak{T}$.

Lemma 3.3. *If there exist five distinct points* $P_{n_5} = [x_{n_5} : y_{n_5}], P_{n_4} = [x_{n_4} : y_{n_4}], P_{n_3} = [x_{n_3} : y_{n_3}], P_{n_2} = [x_{n_2} : y_{n_2}], P_{n_1} = [x_{n_1} : y_{n_1}]$ *of the orbit (3.2), with* $n_5 < n_4 < n_3 < n_2 < n_1 < 0$*, such that*

$$x_{n_i}R_{\mathbb{S}} \neq x_{n_{i+1}}R_{\mathbb{S}} \tag{3.12}$$

for every index $1 \leq i \leq 4$*, then* x_{n_1}/x_{n_2} *is a non zero* $\mathbb{S}$*-integer which is representable, in two essentially different ways, as sum of two* $\mathbb{S}$*-units.*

Proof. Since $\Phi(P_0) = P_0 = [0 : 1]$, from Proposition 2.3, considering $\Phi^{n_i - n_j}$, $P = P_{n_j}$ and $Q = P_0$, it follows that $x_{n_j}|x_{n_i}$ in $R_{\mathbb{S}}$ for all couple of integers $5 \geq j \geq i \geq 1$. Therefore there exist four non zero $T_1, T_2, T_3, T_4 \in R_{\mathbb{S}} \setminus R_{\mathbb{S}}^*$ such that

$$x_{n_i} = T_i x_{n_{i+1}} \text{ for all } i \in \{1, 2, 3, 4\}.$$

From this, for every couple of distinct indexes $1 \leq i < j \leq 5$, it follows that

$$x_{n_i} = T_i \cdot \ldots \cdot T_{j-1} x_{n_j}. \tag{3.13}$$

By Remark 3.1 we have that for all prime ideals $\mathfrak{p} \notin \mathbb{S}$

$$\delta_{\mathfrak{p}}(P_{n_j}, P_O) \geq \min\{\delta_{\mathfrak{p}}(P_{n_j}, P_{n_i}), \delta_{\mathfrak{p}}(P_{n_i}, P_{2n_i - n_j}), \ldots, \delta_{\mathfrak{p}}(P_{m \cdot n_i - (m-1)n_j}, P_0)\} = \delta_{\mathfrak{p}}(P_{n_i}, P_{n_j})$$

for a suitable integer m; thus, by choice of homogeneous coprime coordinates, we observe that $(x_{n_j} y_{n_i} - x_{n_i} y_{n_j})|x_{n_j}$ in $R_{\mathbb{S}}$; in this way by identity (3.13) we deduce that

$$y_{n_i} - T_i \cdot \ldots \cdot T_{j-1} y_{n_j} \in R_{\mathbb{S}}^*.$$

Hence we obtain

$$y_{n_1} - T_1 y_{n_2} = v_1 \tag{3.14}$$
$$y_{n_2} - T_2 y_{n_3} = v_2 \tag{3.15}$$
$$y_{n_1} - T_1 T_2 y_{n_3} = v_3 \tag{3.16}$$
$$y_{n_3} - T_3 y_{n_4} = v_4 \tag{3.17}$$
$$y_{n_2} - T_2 T_3 y_{n_4} = v_5 \tag{3.18}$$
$$y_{n_1} - T_1 T_2 T_3 y_{n_4} = v_6 \tag{3.19}$$
$$y_{n_2} - T_2 T_3 T_4 y_{n_5} = v_7 \tag{3.20}$$
$$y_{n_1} - T_1 T_2 T_3 T_4 y_{n_5} = v_8 \tag{3.21}$$
$$y_{n_3} - T_3 T_4 y_{n_5} = v_9 \tag{3.22}$$
$$y_{n_4} - T_4 y_{n_5} = v_{10}, \tag{3.23}$$

where $v_i \in R_{\mathbb{S}}^*$ for all indexes $1 \leq i \leq 10$.
From (3.15) we deduce that

$$T_2 = \frac{y_{n_2} - v_2}{y_{n_3}}.$$

We put this value of T_2 in (3.16) obtaining

$$y_{n_1} - T_1(y_{n_2} - v_2) = v_3. \tag{3.24}$$

The equation (3.14) tells us that

$$T_1 y_{n_2} = y_{n_1} + v_1.$$

Therefore substituting this value of $T_1 y_{n_2}$ in (3.24) we get

$$T_1 = \frac{v_3}{v_2} - \frac{v_1}{v_2}. \tag{3.25}$$

In the same way from (3.19), (3.14) and (3.18), we obtain

$$T_1 = \frac{v_6}{v_5} - \frac{v_1}{v_5}, \tag{3.26}$$

and from (3.21), (3.14) and (3.20)

$$T_1 = \frac{v_8}{v_7} - \frac{v_1}{v_7}. \tag{3.27}$$

Now we finish the proof by proving that among (3.25), (3.26), (3.27) there exist at least two distinct representations of T_1 as sum of two $\mathbb{S}$-units.
Using the same previous method, from (3.20), (3.15) and (3.22), we obtain that

$$T_2 = \frac{v_7 - v_2}{v_9};$$

therefore $v_7 \neq v_2$ and

$$\left\{\frac{v_3}{v_2}, -\frac{v_1}{v_2}\right\} = \left\{\frac{v_8}{v_7}, -\frac{v_1}{v_7}\right\} \Rightarrow -\frac{v_1}{v_2} = \frac{v_8}{v_7}. \tag{3.28}$$

From (3.20), (3.18) and (3.23), we obtain that

$$T_2 T_3 = \frac{v_7 - v_5}{v_{10}};$$

therefore $v_7 \neq v_5$ and

$$\left\{\frac{v_6}{v_5}, -\frac{v_1}{v_5}\right\} = \left\{\frac{v_8}{v_7}, -\frac{v_1}{v_7}\right\} \Rightarrow -\frac{v_1}{v_5} = \frac{v_8}{v_7}. \tag{3.29}$$

If (3.25), (3.26), (3.27) are the same representation of T_1 as sum of two $\mathbb{S}$-units, then from (3.28) and (3.29) it follows that

$$\left\{\frac{v_3}{v_2}, -\frac{v_1}{v_2}\right\} = \left\{\frac{v_6}{v_5}, -\frac{v_1}{v_5}\right\} = \left\{\frac{v_8}{v_7}, -\frac{v_1}{v_7}\right\} \Rightarrow -\frac{v_1}{v_2} = -\frac{v_1}{v_5} \Rightarrow v_2 = v_5.$$

But this is not possible since from (3.18), (3.15) and (3.17)

$$T_2 = \frac{v_5 - v_2}{v_4} \neq 0.$$

□

Now we use the previous lemma to prove that the set $\{P_{i_r}, \ldots, P_{i_1}, P_{-1}\}$ of all points P_{-j} of the orbit (3.2) such that $x_{-j}R_{\mathbb{S}} \neq x_{-j+1}R_{\mathbb{S}}$ is finite. More precisely we have that $r \leq 3 + 2^{1031\cdot|\mathbb{S}|}$. Indeed, if such five points do not exist we have finished; otherwise for every index $i_{r-2} < i_t \leq i_1$ we apply the previous lemma with $n_1 = -1, n_2 = i_t, n_3 = i_{r-2}, n_4 = i_{r-1}, n_5 = i_r$ obtaining that $x_{-1}/x_{i_t} = uT$ where $T \in \mathfrak{T}$ (the set chosen in Remark 3.2) and u is a suitable $\mathbb{S}$-unit. Therefore

$$P_{i_t} = [x_{-1}/T : uy_{i_t}].$$

In this way we have proved that r is bounded by $3 + |\mathfrak{T}|$. Now it is easy to see that it is possible to choose as bound b for the length of orbits of type (3.2)

$$\left(4 + 2^{1031\cdot|\mathbb{S}|}\right)\left(3 \cdot 7^{4|\mathbb{S}|} + 1\right) + 1$$

which is $< 2^{1045|\mathbb{S}|} - 1$.
Recall that actually we study finite orbits for rational maps with good reduction outside S. Hence we use the bound (1.34) obtaining that we can choose

$$c(s, h_S) = 2^{1045|\mathbb{S}|}\left[12(s+1)\log(5s+5)\right]^{8s}.$$

Now the proof is finished since $|\mathbb{S}| \leq s + h_S - 1$.

3.3 Finiteness of finite orbits

We start by giving three elementary but significant examples in $\mathbb{P}_1(\mathbb{Q})$.

Example 3.1. Suppose that 2 is a S-unit. For every integer $n \geq 1$, let Ψ_n be the rational map defined by

$$\Psi_n(X, Y) = [X((2^n + 1)X - Y)(2^n X - (2^n + 1)Y) : 2^{2n}(X - Y)^3].$$

Ψ_n has good reduction outside S and degree 3. For every $n \geq 1$ we have that $P_{-2} = [1 : 0], P_{-1} = [2^n + 1 : 2^n], P_0 = [0 : 1]$ are three consecutive points of a finite orbit for the rational map Ψ_n since P_0 is a fixed point of Ψ_n. Furthermore, for all primes p, $\delta_p([2^n + 1 : 2^n], [0 : 1]) = v_p(2^n + 1)$, thus there exist infinitely many inequivalent finite orbits, for rational maps with good reduction outside S, in which P_0 is a fixed point.

Example 3.2. For every $y \in \mathbb{Z}$, let Ψ_y be the rational map of degree 2 defined by

$$\Psi_y(X, Y) = [yXY - Y^2 : X^2].$$

Ψ_y has good reduction at every prime. For every $y \in \mathbb{Z}$, the 3-tuple $([1 : y], [0 : 1], [1 : 0])$ is a finite orbit for Ψ_y since $[0 : 1]$ is a periodic point of period 2. Furthermore, for all primes p, $\delta_p([1 : y], [1 : 0]) = v_p(y)$, thus there exist infinitely many inequivalent finite orbits, for rational maps with good reduction at any prime, which contain the cycle $([0 : 1], [1 : 0])$.

Example 3.3. Suppose that 2 is a S-unit. For every integer $n \geq 1$ let Ψ_n be the rational map defined by

$$\Psi_n(X, Y) = [((2^n + 1)X - 2^n Y)Y : (X - Y)(X + 2^n Y)].$$

Ψ_n has god reduction outside S and degree 2. For every $n \geq 1$ we have that the 4-tuple $([2^n : 2^n + 1], [0 : 1], [1 : 1], [1 : 0])$ is a finite orbit for the rational map Ψ_n since $[0 : 1]$ is a periodic point of period 3. Furthermore, for all primes p, $\delta_p([2^n : 2^n + 1], [1 : 0]) = v_p(2^n + 1)$; thus there exist infinitely many finite orbits, for rational maps with good reduction outside S, which contain the cycle $([0 : 1], [1 : 1], [1 : 0])$, of course, as well as for inequivalent finite orbits.

In view of these three examples, it is necessary to fix an n-cycle with $n \geq 4$ in order to obtain a finiteness result.

Proof of Theorem 3.2. Let $n \geq 4$. Let $(P_{-m}, \dots, P_{-1}, P_0, \dots, P_{n-1})$ be a finite orbit in $\mathbb{P}_1(K)$ for a rational map Φ with good reduction outside S, such that $\Phi(P_{n-1}) = P_0$. In this proof we use the ring R_S also if it is not a P.I.D.. Therefore there could not always exist homogeneous coprime S-integral coordinates to represent a point of $\mathbb{P}_1(K)$. But by Proposition 1.1 we represent every point P_i with homogeneous almost coprime S-integral coordinates (x_i, y_i). Thus there exists a constant C, independent on the particular choice of a point in $\mathbb{P}_1(K)$, such that

$$\min\{v_{\mathfrak{p}}(x_i), v_{\mathfrak{p}}(y_i)\} \leq C \tag{3.30}$$

for all prime ideals $\mathfrak{p} \notin S$.

For every prime ideal $\mathfrak{p}$ we have that $\delta_{\mathfrak{p}}(P_0, P_1), \delta_{\mathfrak{p}}(P_0, P_2), \delta_{\mathfrak{p}}(P_0, P_3)$ are fixed finite values, since the cycle $(P_0, P_1, \dots, P_{n-1})$ is fixed. Moreover for every prime ideal $\mathfrak{p} \notin S$ and for all indexes $0 \leq i \leq m$, $1 \leq j \leq 3$, applying Proposition 2.3 to the rational map Φ^i, we deduce that

$$\delta_{\mathfrak{p}}(P_{-i}, P_{-i+j}) \leq \delta_{\mathfrak{p}}(P_0, P_j).$$

Therefore by definition of $\mathfrak{p}$-adic distance and (3.30) we obtain that

$$0 \leq v_{\mathfrak{p}}(x_i y_{i+j} - x_{i+j} y_i) \leq \delta_{\mathfrak{p}}(P_0, P_j) + 2C. \tag{3.31}$$

If $m = 0$ there is nothing to prove. Otherwise P_{-1}, P_0, P_1, P_2 are four distinct points and by the property of cross-ratio (denoted by $\rho(\cdot, \cdot, \cdot, \cdot)$)

$$\rho(P_{-1}, P_0, P_1, P_2) + \rho(P_{-1}, P_0, P_2, P_1) = 1,$$

we have that

$$\frac{(x_{-1}y_1 - x_1y_{-1})(x_0y_2 - x_2y_0)}{(x_{-1}y_0 - x_0y_{-1})(x_1y_2 - x_2y_1)} - \frac{(x_{-1}y_2 - x_2y_{-1})(x_0y_1 - x_1y_0)}{(x_{-1}y_0 - x_0y_{-1})(x_1y_2 - x_2y_1)} = 1 \tag{3.32}$$

Since (3.31) holds for every prime ideal $\mathfrak{p} \notin S$, $i = -1$ and $1 \leq j \leq 3$; there are only finitely many possibilities for

$$v_{\mathfrak{p}}\left(\frac{(x_{-1}y_1 - x_1y_{-1})(x_0y_2 - x_2y_0)}{(x_{-1}y_0 - x_0y_{-1})(x_1y_2 - x_2y_1)}\right); v_{\mathfrak{p}}\left(\frac{(x_{-1}y_2 - x_2y_{-1})(x_0y_1 - x_1y_0)}{(x_{-1}y_0 - x_0y_{-1})(x_1y_2 - x_2y_1)}\right)$$

Therefore we can apply the S-unit equation Theorem obtaining that there exist only finitely many possible values for

$$\frac{x_{-1}y_1 - x_1y_{-1}}{x_{-1}y_0 - x_0y_{-1}}; \frac{x_{-1}y_2 - x_2y_{-1}}{x_{-1}y_0 - x_0y_{-1}}$$

since

$$\frac{(x_0y_2 - x_2y_0)}{(x_1y_2 - x_2y_1)} \text{ and } \frac{(x_0y_1 - x_1y_0)}{(x_1y_2 - x_2y_1)}$$

are fixed.
Now we observe that $(0, 0)$ is the only solution of the system

$$\begin{cases} y_1X + y_0Y = 0 \\ x_1X + x_0Y = 0 \end{cases}$$

since $x_0y_1 - x_1y_0 \neq 0$; hence the identity

$$x_{-1}\left(y_1 - \frac{x_{-1}y_1 - x_1y_{-1}}{x_{-1}y_0 - x_0y_{-1}}y_0\right) = y_{-1}\left(x_1 - \frac{x_{-1}y_1 - x_1y_{-1}}{x_{-1}y_0 - x_0y_{-1}}x_0\right)$$

is not trivial and we deduce that

$$[x_{-1} : y_{-1}] = \left[x_1 - \frac{x_{-1}y_1 - x_1y_{-1}}{x_{-1}y_0 - x_0y_{-1}}x_0 : y_1 - \frac{x_{-1}y_1 - x_1y_{-1}}{x_{-1}y_0 - x_0y_{-1}}y_0\right].$$

This proves that there exist only finitely many possibilities for the point P_{-1}.
Now applying the same method but replacing each index $i \in \{-1, 0, 1, 2\}$ in (3.32) with $i-1$ we obtain the finiteness of possible values for the point P_{-2}. By inductive method we prove this case. Indeed by Theorem 3.1 we have to do only a finite number of steps.
For $n = 2$, if P_{-1}, P_0, P_1 are fixed then $\delta_\mathfrak{p}(P_0, P_1)$ and $\delta_\mathfrak{p}(P_{-1}, P_1)$ are fixed and for all indexes $-m \leq i \leq -1$, $j \in \{1, 3\}$

$$\delta_\mathfrak{p}(P_i, P_{i+j}) \leq \delta_\mathfrak{p}(P_0, P_1)$$

and for $j = 2$

$$\delta_\mathfrak{p}(P_i, P_{i+2}) \leq \delta_\mathfrak{p}(P_{-1}, P_1).$$

For $n = 3$, if P_{-1}, P_0, P_1, P_2 are fixed then $\delta_\mathfrak{p}(P_0, P_1) = \delta_\mathfrak{p}(P_0, P_2)$ and $\delta_\mathfrak{p}(P_{-1}, P_2)$ are fixed and for all indices $-m \leq i \leq -1$, $j \in \{1, 2\}$

$$\delta_\mathfrak{p}(P_i, P_{i+j}) \leq \delta_\mathfrak{p}(P_0, P_1)$$

and for $j = 3$

$$\delta_\mathfrak{p}(P_i, P_{i+3}) \leq \delta_\mathfrak{p}(P_{-1}, P_2).$$

Now we can apply the above cross-ratio method. □

An alternative proof of Theorem 3.2 it can be obtained from the next Lemma which is also useful to prove Theorem 3.3.

Lemma 3.4. *Let n be a fixed integer. For every prime ideal $\mathfrak{p} \notin S$ and for all distinct indexes $0 \leq i < j \leq n-1$ let $\Delta_{\mathfrak{p},i,j}$ be a fixed S-integer. Then there exist only finitely many inequivalent n-tuples $(P_0, P_1, \ldots, P_{n-1}) \in \mathbb{P}_1(K)^n$ such that*

$$\delta_{\mathfrak{p}}(P_i, P_j) = \Delta_{\mathfrak{p},i,j} \tag{3.33}$$

for all $\mathfrak{p} \notin S$ and distinct indexes $0 \leq i < j \leq n-1$.

Proof. It is trivial that if there exist infinitely many prime ideal $\mathfrak{p} \notin S$ such that $\Delta_{\mathfrak{p},i,j} \neq 0$ for some distinct indexes i, j, then n-uples which satisfy condition (3.33) do not exist. Otherwise with the same proof of Proposition 1.2 (which use the Birch-Merriman's result [5]) we prove this lemma. □

Proof of Theorem 3.3. Let $(P_{-m}, \ldots, P_{-1}, P_0)$ be an orbit in $\mathbb{P}_1(K)$ for a rational map Φ with good reduction outside S such that $\Phi(P_0) = P_0$.
If $m = 1$ we have nothing to prove. Otherwise for every index $i \in \{2, \ldots, m\}$, by Proposition 2.3 applied to the rational map Φ^{i-1} and $P = P_{-i}, Q = P_0$ it follows that

$$\delta_{\mathfrak{p}}(P_{-1}, P_0) \geq \delta_{\mathfrak{p}}(P_{-i}, P_0). \tag{3.34}$$

For every integer $i > k > 0$, let l be the maximum integer such that $-i + lk < 0$, applying Remark 3.1 we obtain

$$\delta_{\mathfrak{p}}(P_{-i}, P_0) \geq \min\{\delta_{\mathfrak{p}}(P_{-i}, P_{-i+k}), \delta_{\mathfrak{p}}(P_{-i+k}, P_{-i+2k}), \ldots, \delta_{\mathfrak{p}}(P_{-i+lk}, P_0)\} = \delta_{\mathfrak{p}}(P_{-i}, P_{-i+k})$$

thus by (3.34)

$$\delta_{\mathfrak{p}}(P_{-1}, P_0) \geq \delta_{\mathfrak{p}}(P_{-i}, P_{-i+k}).$$

Now applying Lemma 3.4 and Theorem 3.1 we conclude the proof. □

Bibliography

[1] Apostol T *Introduction to Analytic Number Theory*. Springer-Verlag (1976), New York

[2] Beardon, AF *Iteration of rational functions*. Graduate Texts in Mathematics **132** Springer-Verlag (1991), New York

[3] Benedetto R *Preperiodic points of polynomials over global fields*. ArXiv:math.NT/0506480 (2005)

[4] Beukers F, Schlickewei HP *The equation $x + y = 1$ in finitely generated groups*. Acta Arith **LXXVIII.2** (1996): 189-199

[5] Birch BJ, Merriman JR *Finiteness theorems for binary forms with given discriminant*. Proc London Math Soc (3) **24** (1972): 385-394

[6] Canci JK *Cycles for rational maps of good reduction outside a prescribed set*. Monatsh. Math., to appear.

[7] Canci JK *Finite rational orbits for rational functions*. ArXiv:math.NT/0512338 (2005)

[8] Evertse JH *On equations in S-units and the Thue-Mahler equation*. Invent Math **75** (1984): 561-584

[9] Evertse JH *On sums of S-units and linear recurrences*. Compositio Math **53** no 2 (1984): 225-244

[10] Evertse JH, Győry K *Effective finiteness results for binary forms with given discriminant*. Compositio Math **79** (1991): 169-204

[11] Evertse JH *The number of solutions of decomposable form equations*. Invent Math **122** (1995): 559-601

[12] Furstenberg H *Recurrence in ergodic theory and combinatorial number theory*. M. B. Porter Lectures, Princeton University Press, Princeton, N.J., (1981)

[13] Halter-Koch F, Narkiewicz W *Scarcity of finite polynomial orbits*. Publ Math Debrecen **56/3-4** (2000): 405-414

[14] Halter-Koch F, Narkiewicz W *Polynomial cycles and dynamical units*. Proc. Conf. Analytic and Elementary Number Theory, Wien 1997: 70-80

[15] Halter-Koch F, Narkiewicz W *Polynomial cycles in Finitely Generated Domain*. Monatsh. Math. **119** (1997): 275-279

[16] Hartshorne R *Algebraic Geometry*. Springer-Verlag (1977) New York

[17] Hindry M, Silverman JH *Diophantine Geometry: An Introduction*. Springer-Verlag, GTM **201** (2000)

[18] Lang S *Algebraic number theory*. Springer-Verlag, GTM **110** (1986)

[19] Lang S *Algebra*. Springer-Verlag, Graduate Texts in Mathematics **211** (2002) New York

[20] Marcus DA *Number Fields*. Springer-Verlag, Universitext (1977)

[21] Milnor J *Dynamics in one complex variable. Introductory lectures*. Friedr. Vieweg & Sohn (1999)

[22] Morton P, Silverman JH *Rational Periodic Points of Rational Functions*. Inter Math Res Notices **2** (1994): 97-110

[23] Morton P, Silverman JH *Periodic points, multiplicities, and dynamical units*. J Reine Angew Math **461** (1995): 81-122

[24] Narkiewicz W *Polynomial cycles in algebraic number fields*. Colloq Math **58** (1989): 151-155

[25] Narkiewicz W, Pezda T *Finite polynomial orbits in finitely generated domain*. Monatsh. Math. **124** (1997): 309-316

[26] Northcott DG *Periodic points of an algebraic variety*. Ann. of Math. (2) **51** (1950): 167-177

[27] Pezda T *Polynomial cycles in certain local domains*. Acta Arith **LXVI:1** (1994): 11-22

[28] Pezda T *Cycles of polynomial mappings in several variables*. Manuscripta Math. **83** (1994): 279-289

[29] Pezda T *Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals*. Acta Arith. **108-2** (2003): 127-146

[30] Pezda T *Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals. II*. Monatsh. Math. **145-4** (2005): 321-331

[31] Serre JP *Lectures on the Mordell-Weil Theorem*. Friedr. Vieweg & Sohn. Brauschweig (1989)

[32] Siegel CL *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \ldots + k$. J. London Math. **1** (1926)

[33] Silverman JH *Integer points, Diophantine approximation, and iteration of rational maps*. Duke Math. J. **71/3** (1993): 793-829

[34] Silverman JH, Tate J *Rational points on elliptic curves*. Springer-Verlag, Undergraduate Texts in Mathematics, (1992)

[35] van der Poorten AJ, Schlickewei HP *The growth condition for recurrence sequences*. Rep. No. 82-0041, Dept. Math., Macquarie Univ., North Ryde, Australia (1982)