ABSTRACT

Title of dissertation: ARITHMETIC DYNAMICS OF QUADRATIC POLYNOMIALS AND DYNAMICAL UNITS

Chatchawan Panraksa, Doctor of Philosophy, 2011

Dissertation directed by: Professor Lawrence C. Washington
Department of Mathematics

The arithmetic dynamics of rational functions have been studied in many contexts. In this thesis, we concentrate on periodic points. For $\phi(x) = x^2 + c$ with c rational, we give a parametrization of all points of order 4 in quadratic fields. For a point of order two and a point of order three for a rational function defined over a number field with good reduction outside a set S, it is known that the bilinear form $B([x_1, y_1], [x_2, y_2]) = x_1y_2 - x_2y_1$ yields a unit in the ring of S-integers of a number field. We prove that this is essentially the only bilinear form with this property. Finally, we give restrictions on the orders of rational periodic points for rational functions with everywhere good reduction.

ARITHMETIC DYNAMICS OF QUADRATIC POLYNOMIALS AND DYNAMICAL UNITS

by

Chatchawan Panraksa

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2011

Advisory Committee:

Professor Lawrence C. Washington, Chair/Advisor
Professor McBlaine M. Boyle
Professor William I. Gasarch
Professor Niranjan Ramachandran
Professor Harry Tamvakis

DEDICATION

To my parents, Sopana and Pradub, and my wife, Patcharee.

ACKNOWLEDGEMENTS

It would be impossible to finish my dissertation without guidance of my committee members, help from friends, and support from my family and wife.

First and foremost, I would like to gratefully and sincerely thank my advisor, Professor Lawrence C. Washington, for his guidance, caring, understanding, patience. His mentorship was paramount in providing a well rounded experience for my long-term career goals.

I would like to thank my parents, Sopana and Pradub Panraksa, and my brother Tanapat Panraksa for all their support throughout my life.

Finally I would like to thank my wife, Patcharee Panraksa. She was always there cheering me up and stood by me through the good and bad times.

TABLE OF CONTENTS

Chapter 1

Introduction

In this thesis, we study arithmetic questions arising from discrete dynamical systems. The techniques used draw on algebraic number theory and algebraic geometry.

1.1 Discrete Dynamical Systems

A discrete dynamical system is simply a set X with a self-map $\phi : X \to X$, allowing for iteration. For a non-negative integer n, denote by ϕ^n the n^{th} iterate of ϕ under composition, with ϕ^0 taken to be the identity map. In classical complex dynamics, the set X is the Riemann sphere $\mathbb{P}^1(\mathbb{C})$. A morphism is a map given by

$$\pi : (x_1, ..., x_m) \mapsto (f_1(x_1, ..., x_m), ..., f_n(x_1, ..., x_m))$$

where the f_i are polynomials. More generally for this thesis, let K be a field with algebraic closure $\overline{K}$. Let $\phi : \mathbb{P}^1(\overline{K}) \to \mathbb{P}^1(\overline{K})$ be a morphism defined over K; then we may write $\phi(z) \in K(z)$ as a rational map: $\phi(z) = F(z)/G(z)$, $F, G \in K[z]$, $\gcd(F, G) = 1$, $\deg \phi = \max\{\deg F, \deg G\}$.

The (forward) orbit of a point $\alpha \in \mathbb{P}^1$ under ϕ is simply the set of iterates of α:

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

A fundamental problem in dynamics is to classify points according to their orbits. Some types of points are of particular interest. A point $\alpha \in \mathbb{P}^1$ is *periodic* if there exists an integer $n > 0$ such that $\phi^n(\alpha) = \alpha$, and α is *preperiodic* if there exist integers $n > m \geq 0$ such that $\phi^n(\alpha) = \phi^m(\alpha)$:

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

$$\mathrm{PrePer}(\phi, \mathbb{P}^1) = \{\alpha \in \mathbb{P}^1 : \phi^n(\alpha) = \phi^m(\alpha) \text{ for some } n > m \geq 0\}.$$

We say P has period n if $\phi^n(P) = P$, and it has *primitive* period n if $n > 0$ is the smallest such integer.

1.2 Arithmetic Questions

One type of arithmetic question arising from discrete dynamical systems is the analysis of $\mathrm{PrePer}(\phi, K)$, the preperiodic points of a map $\phi(z) \in K(z)$ lying in the field K. Northcott proved in [18] that for a fixed morphism $\phi : \mathbb{P}^N(\overline{K}) \to \mathbb{P}^N(\overline{K})$ of degree at least 2 defined over a number field K, there are at most finitely many preperiodic points in $\mathbb{P}^N(K)$. Lying deeper is the uniform boundedness conjecture of Morton and Silverman (see [14]).

Conjecture 1. *Let $K/\mathbb{Q}$ be a number field of degree D, and let $\phi : \mathbb{P}^N(\overline{K}) \to \mathbb{P}^N(\overline{K})$ be a morphism of degree $d \geq 2$ defined over K. There is a constant $\kappa(D, N, d)$ such that*

$$\#PrePer(\phi, K) \leq \kappa(D, N, d).$$

This conjecture implies, for example, the uniform boundedness for torsion points on abelian varieties over number fields (see [7]). Even the special case $n = 1$ and $d = 4$ is enough to imply Merel's uniform boundedness of torsion points on elliptic curves proved in [12]. Torsion points on elliptic curves are exactly preperiodic points under the multiplication-by-2 map on the curve. Points on the elliptic curve map to $\mathbb{P}^1$ via their x-coordinate, and this multiplication-by-2 map induces a degree-four rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$, with the x-coordinates of the torsion points mapping to preperiodic points of ϕ.

1.3 Dynatomic Polynomials

To tackle these arithmetic questions, we require algebraic descriptions of periodic and preperiodic points. For any $\phi(z) \in K(z)$, there is a homogeneous polynomial $\Phi_{n,\phi}(x, y) \in K[x, y]$ whose roots are precisely points of period dividing n for ϕ, where (x, y) is a homogeneous coordinate of z. If we homogenize $\phi(z) = \frac{F(z)}{G(z)}$ to $\phi(x, y) = [F(x, y) : G(x, y)]$ and write $\phi^n(x, y) = [F_n(x, y) : G_n(x, y)]$, then

$$\Phi_{n,\phi} = yF_n(x, y) - xG_n(x, y).$$

If $P = [x : y]$ is a root of this polynomial, then by construction $\phi^n(P) = P$.

The polynomial Φ_n has as its roots all points of period n, including those of primitive period $k < n$ but satisfying $k \mid n$. We would like to examine points of primitive period n, so we define the n^{th} *dynamical polynomial* for ϕ by

$$\Phi^*_{n,\phi}(x,y) = \prod_{k|n} (\Phi_{k,\phi}(x,y))^{\mu(n/k)} = \prod_{k|n} (yF_k(x,y) - xG_k(x,y))^{\mu(n/k)},$$

where μ is the Moebius mu function. It is not clear *a priori* that $\Phi^*_n(x,y)$ is a polynomial, but this is in fact the case. The roots of $\Phi^*_n(x,y)$ are points of formal period n, which include all points of primitive period n. We say that P has *formal period* n if $\Phi^*(P) = 0$. It is clear that

$$\text{primitive period} \quad n \Rightarrow \text{formal period} \quad n \Rightarrow \text{period} \quad n,$$

but neither of the reverse implications is true in general (see [23] p.148-149).

1.4 Quadratic Polynomials

Let $\phi(z) \in K[z]$ be a quadratic polynomial, and assume that char $K \neq 2$. Then $\phi(z)$ is linearly conjugate over K to some map $f_c(z) = z^2 + c$ with $c \in K$. To see this, write

$$\phi(z) = Az^2 + Bz + C, \quad A, B, C \in K.$$

Conjugating by $h(z) = (2z - B)/(2A) \in PGL_2(K)$, we get

$$\phi^h(z) = z^2 + \underbrace{(AC - \frac{1}{4}B^2 + \frac{1}{2}B)}_{c \in K}.$$

Thus, studying the dynamics of quadratic polynomials–including the arithmetic dynamics of these maps–reduces to studying the dynamics of the one-parameter family $f_c(z) = z^2 + c$. This is certainly the most-studied family of rational maps. The famous Mandelbrot set is a subset of the c-parameter plane for f_c, describing the fate of $\mathcal{O}_{f_c}(0)$.

We now summarize some of the arithmetic results known for the family f_c. In his thesis, Bousch [1] proved the following.

1. $\Phi^*_{n,f_c}(z) = \Phi^*_n(z,c) \in \mathbb{Z}[z,c]$, and this polynomial is irreducible for every n.

2. The affine curve $Y_1(n)$ given by $\Phi^*_n(z,c) = 0$ is smooth.

3. Let $X_1(n)$ be the normalization of the projective closure of $Y_1(n)$. Then

$$\text{genus } X_1(n) = 1 + \frac{n-3}{4}\kappa(n) - \frac{1}{4}\sum_{m|n} \phi(\frac{m}{n}) m\kappa(m)$$

   where $\kappa(n) = \sum_{k|n} \mu(n/k)2^k$ ($\kappa(n)$ is essentially the z-degree of Φ^*_n) and ϕ is the Euler totient function.

Bousch's genus formula shows that $X_1(1), X_1(2)$, and $X_1(3)$ are all rational. So there are one-parameter families of c-values giving maps f_c with rational fixed points, rational points of period 2, and rational points of period 3, respectively.

The genus of $X_1(4)$ is 2, and in [13] Morton shows that this curve is birational to the elliptic modular curve $X_1(16)$, and that it has no rational points. In other words, there are no quadratic polynomials defined over $\mathbb{Q}$ with a rational point of primitive period 4. $X_1(5)$ has genus 14. This curve is not modular, but in [8] Flynn, Poonen, and Shaefer show that there are no finite rational points. So there are no quadratic polynomials defined over $\mathbb{Q}$ with a rational point of primitive period 5.

In [19] Poonen conjectures that no quadratic polynomial ϕ defined over $\mathbb{Q}$ has rational points of primitive period $n > 3$. He shows that if the conjecture is true, then for such maps,

$$\#\mathrm{PrePer}(\phi, \mathbb{Q}) \leq 9.$$

The set $\mathrm{PrePer}(\phi, K)$ of preperiodic point of ϕ defined over K can be represented by a directed graph, with an arrow from P to $\phi(P)$, and Poonen provides a complete analysis of directed graphs that occur as $\mathrm{PrePer}(\phi, \mathbb{Q})$ for points of primitive period $n \leq 3$ and $\phi \in \mathbb{Q}[x]$ a quadratic polynomial.

1.5 Summary of the Results

In Chapter 2, we consider the 4-cycles of quadratic polynomials. Morton proves in [13] that there are no rational values of c for which the quadratic map $f(x) = x^2+c$ has a rational 4-cycle. However, Flynn, Poonen, Schaefer give an example in [8]: $\phi(x) = x^2 - \frac{31}{48}$ has a 4-cycle over a quadratic field $\mathbb{Q}(\sqrt{-15})$ described by the following diagram

$$\frac{1}{4} + \frac{\sqrt{-15}}{6} \to -1 + \frac{\sqrt{-15}}{12} \to \frac{1}{4} - \frac{\sqrt{-15}}{6} \to -1 - \frac{\sqrt{-15}}{12} \to \frac{1}{4} + \frac{\sqrt{-15}}{6}.$$

We generalize this example to the following result:

Theorem 1.5.1. *Let $\{x_1, x_2, x_3, x_4\}$ be a 4-cycle for the quadratic polynomial $\phi(x) = x^2 + c$, where $c \in \mathbb{Q}$. If x_i's are in a quadratic field, then x_1 and x_3 are Galois conjugates.*

Parametrization of 4-cycles was proved by Netto, Erkama and Morton (see [6, 13, 17]) using Galois theory. We show this result by a different approach, namely Groebner bases. Moreover, equipped with Theorem 1.5.1, for $c \in \mathbb{Q}$ we can generate all 4-cycles over quadratic fields.

Theorem 1.5.2. *Let $\phi(z) = z^2 + c$. Then*

(a) *c and the points of period 4 can be parametrized over $\mathbb{C}$ by the following:*

$$c = \frac{1 - 4t^3 - t^6}{4t^2(t^2 - 1)},$$

$$x_1 = \frac{t^4 - t^2 + \sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)}, x_2 = \frac{1 - t^2 + t\sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)},$$

$$x_3 = \frac{t^4 - t^2 - \sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)}, x_4 = \frac{1 - t^2 - t\sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)},$$

where $t = x_1 + x_3$.

(b) *Assume that $c \in \mathbb{Q}$ and x_1, x_2, x_3, x_4 lie in a quadratic field, then $t \in \mathbb{Q}$. Therefore, as t ranges through $\mathbb{Q}$, we obtain all 4-cycles over quadratic fields.*

Another interesting result in arithmetic dynamics is that we can use periodic points of rational functions to produce units, called *dynamical units*, over fields with valuations (see [15]). In Chapter 3, we will consider the converse problems of the results in [15]. To be more precise we consider the following question:

What are the forms that can produce units from periodic points of rational functions?

We prove that, under certain conditions, the form is unique.

Theorem 1.5.3. *Let K be number field and let T be a finite set of places of K that includes the archimedean places. Let $\widetilde{T}$ be the set of places of $\overline{\mathbb{Q}}$ lying above the places in T. Suppose $a, b, c, d \in K$ are such that*

$$B([x_1, y_1], [x_2, y_2]) = ax_1x_2 + bx_1y_2 + cx_2y_1 + dx_2y_2$$

is a $\widetilde{T}$-unit whenever ϕ is a rational function of degree at least 2 defined over K with everywhere good reduction, $[x_1, y_1] \in \mathbb{P}^1(\overline{\mathbb{Q}})$ is a normalized point of order 2 and $[x_2, y_2] \in \mathbb{P}^1(\overline{\mathbb{Q}})$ is a normalized point of order 3 for ϕ. Then $a = 0 = d$ and $b = -c$. Moreover, b, c are T-units.

Morton and Silverman prove in [14] that for $\phi(x) \in \mathbb{Q}(z)$ with good reduction at 2 and 3, if $\phi(x)$ has a rational primitive n-cycle, then $n \mid 24$. We will use dynamical units (with a stronger assumption) to give an improved bound.

Theorem 1.5.4. *Let $\phi \in \mathbb{Q}(z)$ with good reduction everywhere (outside ∞). Assume that ϕ has a rational n-cycle. Then $n \mid 6$.*

Chapter 2

Rational Periodic Points

2.1 Rational Periodic Points of Quadratic Polynomials

Polynomials $\phi(z), \varphi(z) \in \mathbb{Q}[z]$ are *linearly conjugate* over $\mathbb{Q}$ if there exists a linear polynomial $l(z) \in \mathbb{Q}[z]$ such that $l(\phi(l^{-1}(z))) = \varphi(z)$. In this case, l maps the rational preperiodic points of $\phi(z)$ bijectively to the rational preperiodic points of $\varphi(z)$, also preserving the graph that describes the cycles and preperiodic points. Every quadratic polynomial in $\mathbb{Q}[z]$ is linearly conjugate over $\mathbb{Q}$ to one of the form $z^2 + c$ with $c \in \mathbb{Q}$, so from now on, it is sufficient to consider $\phi(z) = z^2 + c$. In the subsequent theorems for polynomials, we disregard ∞, which is always a rational fixed point.

Theorem 2.1.1. *[19], [21] Let $\phi(z) = z^2 + c$ with $c \in \mathbb{Q}$. Then*

1. $\phi(z)$ has a rational point of period 1 (i.e., a rational fixed point) if and only if $c = 1/4 - \rho^2$ for some $\rho \in \mathbb{Q}$. In this case, there are exactly two, $1/2 + \rho$ and $1/2 - \rho$, unless $\rho = 0$, in which case they coincide.

2. $\phi(z)$ has a rational point of period 2 if and only if $c = -3/4 - \sigma^2$ for some $\sigma \in \mathbb{Q}$, $\sigma \neq 0$. In this case, there are exactly two, $-1/2 + \sigma$ and $-1/2 - \sigma$ (and these form a 2-cycle).

3. $\phi(z)$ has a rational point of period 3 if and only if

$$c = -\frac{\tau^6 + 2\tau^5 + 4\tau^4 + 8\tau^3 + 9\tau^2 + 4\tau + 1}{4\tau^2(\tau+1)^2}$$

for some $\tau \in \mathbb{Q}, \tau \neq -1, 0$. In this case, there are exactly three,

$$x_1 = \frac{\tau^3 + 2\tau^2 + \tau + 1}{2\tau(\tau+1)},$$
$$x_2 = \frac{\tau^3 - \tau - 1}{2\tau(\tau+1)},$$
$$x_3 = \frac{\tau^3 + 2\tau^2 + 3\tau + 1}{2\tau(\tau+1)}$$

and these are cyclically permuted by $\phi(z)$.

Theorem 2.1.2. *[19] Let $\phi(z) = z^2 + c$ with $c \in \mathbb{Q}$. Then*

1. $\phi(z)$ has both rational points of period 1 and rational points of period 2 if and only if

$$c = -\frac{3\mu^4 + 10\mu^2 + 3}{4(\mu^2-1)^2}$$

for some $\mu \in \mathbb{Q}, \mu \neq -1, 0, 1$. In this case the parameters ρ and σ of Theorem 2.1.1 are

$$\rho = -\frac{\mu^2+1}{\mu^2-1}, \rho = \frac{2\mu}{\mu^2-1}.$$

2. If $\phi(z)$ has rational points of period 3, it cannot have any rational points of period 1 or 2.

2.2 Parametrization of Periodic Points

Parametrization of 4-cycles was proved by Netto, Erkama and Morton (see [6, 13, 17]) using Galois theory. We will show this result by different approach; namely Groebner bases.

Theorem 2.2.1. *Let $\phi(z) = z^2 + c$. Then c and the points of period 4 can be parametrized over $\mathbb{C}$ by the following:*

$$c = \frac{1 - 4t^3 - t^6}{4t^2(t^2 - 1)},$$

$$x_1 = \frac{t^4 - t^2 + \sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)}, \qquad x_2 = \frac{1 - t^2 + t\sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)},$$

$$x_3 = \frac{t^4 - t^2 - \sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)}, \qquad x_4 = \frac{1 - t^2 - t\sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)},$$

where $t = x_1 + x_3$.

Proof. We will solve the system of equations generated by periodic points of quadratic functions by the means of Groebner bases. Let $\phi(x) = x^2 + c$, $\phi(x_1) = x_2$, $\phi(x_2) = x_3$, $\phi(x_3) = x_4$, $\phi(x_4) = x_1$, $t = x_1 + x_3$. Assume that x_1 is of primitive period 4. Recall that the 4^{th} *dynatomic polynomial* of $\phi(x)$ is

$\Phi_4^*(x) = x^{12} + 6cx^{10} + x^9 + (3c + 15c^2)x^8 + 4cx^7 + (1 + 12c^2 + 20c^3)x^6 + (2c + 6c^2)x^5 + (15c^4 + 3c^2 + 4c + 18c^3)x^4 + (1 + 4c^2 + 4c^3)x^3 + (6c^3 + 6c^5 + 12c^4 + c + 5c^2)x^2 + (c^4 + c^2 + 2c + 2c^3)x + 2c^2 + c^6 + 1 + 3c^3 + 3c^5 + 3c^4$

and $\Phi_4^*(x) = 0$ if and only if x is a point of primitive period 4. Let G be the ideal in $\mathbb{C}[x_1, x_3, c, t]$ generated by $\{\phi(\phi(x_1)) - x_3, \Phi_4^*(x_1), t - (x_1 + x_3)\}$. Then the Groebner basis with the lexicographic ordering (x_3, x_1, t, c), i.e., $x_3 > x_1 > t > c$ is $B_1 = \{-1 + 4t^3 - 4ct^2 + 4t^4c + t^6, 2c - 4ct + 5t^2 - 2tx_1 + 2x_1^2 + 4t^3c + t^5, -t + x_1 + x_3\}$. We may observe that B_1 contains a bivariate polynomial, $-1 + 4t^3 - 4ct^2 + 4t^4c + t^6$, which yields

$$c = \frac{1 - 4t^3 - t^6}{4t^2(t^2 - 1)}.$$

To find the parametrization of x_1, we will reorder the lexicography. The corresponding Groebner basis with respect to the lexicographic ordering (x_3, c, t, x_1), i.e., $x_3 > c > t > x_1$, is $B_2 = \{1-2t^3-2t-4t^2x_1^2+4x_1t^3-2t^4+4t^4x_1^2-4t^5x_1+t^6, 2+2x_1^2-2tx_1+3t^2+2c+4tx_1^2-4t^2x_1+2t^3-4t^3x_1^2+4t^4x_1-t^5, -t+x_1+x_3\}$. We may again observe that B_2 contains a bivariate polynomial: $1-2t^3-2t-4t^2x_1^2+4x_1t^3-2t^4+4t^4x_1^2-4t^5x_1+t^6$. It follows that

$$x_1 = \frac{t^4 - t^2 + \sqrt{(t^4-1)(t^2+2t-1)}}{2t(t^2-1)}.$$

Since we can parametrize c and x_1, by applying ϕ, we can also parametrize x_2, x_3 and x_4. $\square$

In [13] Morton shows that there is no rational point of primitive period 4 for quadratic polynomials $p(x) \in \mathbb{Q}$. We state his result as the following theorem:

Theorem 2.2.2. *[13] There are no finite rational solutions* (x, c) *of the equation* $\Phi_4^*(x, c) = 0$*. In other words, there are no rational values of* c *for which the quadratic map* $f(x) = x^2 + c$ *has a rational 4-cycle.*

However, by Theorem 2.2.1 there are infinitely many quadratic 4-cycles for $c \in \mathbb{Q}$. We investigate this in the next section.

2.3 Points of Period 4 in Quadratic Fields

By Theorem 2.2.1, it is easy to see that if $t \in \mathbb{Q}$, then $c \in \mathbb{Q}$ and x_1, x_3 (also x_2, x_4) are Galois conjugate. However, it is not obvious that this is true without the rationality of t. In the following we will prove that it is the case. For $c = 0$, the dynatomic polynomial of $\phi(x) = x^2$ is $x^{12} + x^9 + x^6 + x^3 + 1$ which has no quadratic roots. For the rest of this chapter we will assume that $c \neq 0$.

Lemma 2.3.1. *Let x_i's be periodic points of period 4 for the quadratic polynomial $\phi(x) = x^2 + c$, where $c \in \mathbb{Q}$. If $\bar{x}_1 \neq x_3$, then $\{x_1, x_2, x_3, x_4\} \cap \{\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4\} = \emptyset$.*

Proof. Assume to the contrary that $\{x_1, x_2, x_3, x_4\} \cap \{\bar{x}_1, \bar{x}_2, \bar{x}_3, \bar{x}_4\} \neq \emptyset$. If x_i is in the intersection, then applying ϕ the appropriate number of times shows that x_1 is in the intersection. In [13] Morton proved that there is no rational point of period 4 for $\phi(x) = x^2 + c$. This implies that $\overline{x}_1 \neq x_1$. Assume that $\overline{x}_1 = x_2$. Then $\bar{x}_3 = \overline{\phi(\phi(x_1))} = \phi(\bar{x}_2) = \phi(x_1) = x_2 = \bar{x}_1$. Therefore, $x_1 = x_3$, contradiction.
If $\overline{x}_1 = x_4$, then $\overline{x}_2 = \phi(\overline{x}_1) = \phi(x_4) = x_1$, which we just proved cannot happen. □

Let $c \in \mathbb{Q}$ and $\phi(X) = X^2 + c$. Let x be a point of primitive period 4. We let z be the trace of x: $z = (1 + \phi + \phi^2 + \phi^3)(x)$. A straightforward computation shows that

$$z = x^8 + 4cx^6 + (1 + 2c + 6c^2)x^4 + (1 + 2c + 4c^2 + 4c^3)x^2 + x + 3c + 2c^2 + 2c^3 + c^4.$$

By computation, $c = \dfrac{(-z^3 - 3z - 4)}{4z}$ (see [13]).
By factoring $\Phi_4^*(x, c) = \Phi_4^*(x, \dfrac{(-z^3 - 3z - 4)}{4z})$ we find that x is a root of the polynomial

$$\begin{aligned} p_z(X) :&= p(X, z) \\ &= X^4 - zX^3 - \frac{z^2 + 3z + 4}{2z}X^2 + \frac{z^3 + 2z^2 + 5z + 8}{4}X \\ &\quad - \frac{z^6 + 2z^5 + 4z^4 + 6z^3 - 5z^2 - 8z - 16}{16z^2} \end{aligned}$$

(this polynomial is computed in [13]).

Lemma 2.3.2. *Let $c \in \mathbb{C}$. Let z_1, z_2, z_3 be the roots of $z^3 + (4c+3)z + 4 = 0$. Then the four roots of the polynomial $p_j(X) = p_{z_j}(X)$, for $j = 1, 2, 3$ form an orbit of $\phi(X) = X^2 + c$.*

Proof. Let $j \in \{1, 2, 3\}$ Note that it is possible for $p_j(X) \notin \mathbb{Q}[X]$. Let x_1 be a 4-periodic point of $\phi(X)$ and a root of $p_j(X)$. A calculation shows that $p_j(\phi(X)) = p_j(X)p_j(-X)$. Therefore, $p_j(\phi(x_1)) = 0$. This implies that $\phi(x_1)$ is also a root of $p_j(X)$. Since $p_j(X)$ is of degree 4 and x_1 is a 4-periodic point of $\phi(X)$, the roots of $p_j(X)$ are the orbit generated by x_1. □

Let $D(f)$ denote the discriminant of the polynomial f and let $R(f, g)$ denote the resultant of polynomials f and g.

Lemma 2.3.3. *Let f, g and h be monic polynomials. Then*

$$D(fg) = D(f)D(g)R^2(f, g)$$

and

$$D(fgh) = D(f)D(g)D(h)R^2(f, g)R^2(g, h)R^2(h, f).$$

Proof. See [20] pp.23-24. □

Theorem 2.3.4. *Let $\{x_1, x_2, x_3, x_4\}$ be a 4-cycle for the quadratic polynomial $\phi(x) = x^2 + c$, where $c \in \mathbb{Q}$. If x_i's are in a quadratic field, then x_1 and x_3 are Galois conjugates.*

Proof. Assume that x_1 and $x_3 = \phi(\phi(x_1))$ are not Galois conjugates. Since $c \in \mathbb{Q}$, the Galois conjugates of x_i's, called $\bar{x}_i$'s, must also be periodic points of $\phi(X)$.

By Lemma 2.3.2, the dynatomic polynomial of $\phi(X)$ is of the form $\Phi_4^*(X) = p_1(X)p_2(X)p_3(X)$, where the roots of each $p_i(X)$ form an orbit. Assume that the roots of $p_1(X)$ are x_1, x_2, x_3, x_4. By Lemma 2.3.1, these roots are disjoint from $\overline{x_1}, \overline{x_2}, \overline{x_3}, \overline{x_4}$. Without loss of generality, we may assume these are the roots of $p_2(X)$. Let z_j be the coefficient of X^3 in $p_j(X)$ for $j = 1, 2, 3$. Thus, z_1 and z_2 are conjugate. By Lemma 2.3.3,

$$D(p_1(X)p_2(X)) = D(p_1(X))D(p_2(X))R^2(p_1(X), p_2(X)).$$

Since $R(p_1(X), p_2(X)) = \prod(x_i - \bar{x}_j)$,

$$\begin{aligned}\overline{R(p_1(X), p_2(X))} &= (-1)^{16}R(p_1(X), p_2(X)) \\ &= R(p_1(X), p_2(X)).\end{aligned}$$

Thus, $R(p_1(X), p_2(X)) = r \in \mathbb{Q}$. A calculation shows that

$$D(p_j(X)) = \frac{(z_j + 2)^2(z_j^2 + 4)^3}{z_j^4},$$

for $j = 1, 2$. Note that $p_1(X)p_2(X)$ can be written as

$$p_1(X)p_2(X) = q_1(X)q_2(X)q_3(X)q_4(X),$$

where $q_i(X) = (X - x_i)(X - \bar{x}_i)$ for $i = 1, 2, 3, 4$ are rational quadratic polynomials (and their roots lie in the same quadratic field.) Therefore, $D(q_i) = ds_i^2, i = 1, 2, 3, 4,$ with $d, s_i \in \mathbb{Q}$. This implies that

$$\begin{aligned}D(p_1(X)p_2(X)) &= D(q_1(X)q_2(X)q_3(X)q_4(X)) \\ &= d^4s_1^2s_2^2s_3^2s_4^2R^2,\end{aligned}$$

where R is a product of resultants of q_i's. The above implies that

$$D(p_1(X)p_2(X)) = \frac{(z_1+2)^2(z_1^2+4)^3}{z_1^4}\frac{(z_2+2)^2(z_2^2+4)^3}{z_2^4}r^2.$$

Since z_1 and z_2 are quadratic conjugate, $\dfrac{(z_1+2)(z_1^2+4)}{z_1^2}\dfrac{(z_2+2)(z_2^2+4)}{z_2^2} \in \mathbb{Q}$. It follows that $(z_1^2+4)(z_2^2+4) = s^2$, for some $s \in \mathbb{Q}$.

Since z_i's satisfy $h(Z) = Z^3 + (4c+3)Z + 4 = 0$, we have $z_1 + z_2 + z_3 = 0$ and $z_1 z_2 z_3 = -4$. Since z_1 and z_2 are quadratic conjugate, $u = z_1 z_2$ and $v = z_1 + z_2$ are rational. Note that $z_3 = -(z_1 + z_2) = -v$. This implies that $uv = -z_1 z_2 z_3 = 4$. Thus,

$$\begin{aligned} s^2 &= (z_1^2+4)(z_2^2+4). \\ &= u^2 + 4(v^2 - 2u) + 16 \\ &= u^2 + 4(\frac{16}{u^2} - 2u) + 16. \end{aligned}$$

This becomes $u^4 - 8u^3 + 16u^2 + 64 = t^2$ for some $t \in \mathbb{Q}$. This changes to an elliptic curve with equation $y^2 = x^3 + x^2 - x$ (see [25], pages 37-38), which has 6 torsion points generated by $(-1, 1)$ (namely, $\{(-1, \pm 1), (1, \pm 1), (0, 0), \infty\}$.) This is the whole Mordell-Weil group (see [3], pages 110). The corresponding u, v are $u = \frac{16(x+16)}{y}$ and $v = -8 + \frac{u^2 x}{16}$. Thus, $u = 0, 4$. Since $uv = 4$, $u = 4$ and $v = 1$. The only values of z_j's are $(1 + \sqrt{-15})/2$ and its conjugate. However, when $z_j = (1 \pm \sqrt{-15})/2$ we have $c = \frac{-z^3-3z-4}{4z} = 0$, contradiction. Thus, x_1 and $x_3 = \phi(\phi(x_1))$ are Galois conjugate. $\square$

The Theorem 2.3.4 can be used to consider factors of $\Phi_4^*(x) = \Phi_4^*(x, c)$ for $c \in \mathbb{Q}$. We have a partial result on the factorization of $\Phi_4^*(x)$ by the following theorem.

Theorem 2.3.5. *For $c \in \mathbb{Q}$ the dynatomic polynomial $\Phi_4^*(x) = \Phi_4^*(x, c)$ cannot be factored in $\mathbb{Q}[X]$ as $\{2, 2, 2, 2, 4\}$, i.e., a product of four quadratic and one (not necessarily irreducible) quartic polynomials.*

Proof. Assume to the contrary that the 4^{th} dynatomic polynomial $\Phi_4^*(X)$ can be factored as $\Phi_4^*(X) = q_1(X)q_2(X)q_3(X)q_4(X)r(X)$, when q_i's are quadratic polynomials and $r(X)$ is a quartic polynomial (not necessarily irreducible). By Theorem 2.2.2, q_i's are irreducible. Let x_1 be a 4-periodic point of $\phi(X)$ over a quadratic field. Let $x_2 = \phi(x_1)$, $x_3 = \phi^2(x_1)$ and $x_4 = \phi^3(x_1)$. Without loss of generality, assume that $q_1(x_1) = 0$. By Theorem 2.3.4, $q_1(x_3) = 0$. Similarly, we can assume that $q_2(x_2) = 0 = q_2(x_4)$. Now assume that x_1' is a root of $q_3(X)$. Let $x_2' = \phi(x_1')$, $x_3' = \phi^2(x_1')$ and $x_4' = \phi^3(x_1')$. Then $q_3(x_1') = 0 = q_3(x_3')$ and $q_4(x_2') = q_4(x_4')$. Note that the x_i's lie in the same quadratic field and the x_i''s also lie in the same quadratic field (possibly different from the one containing x_i's). It follows that $D(q_1)D(q_2) = s_1^2$ and $D(q_3)D(q_4) = s_2^2$, for some $s_1, s_2 \in \mathbb{Q}$. Now let $p_1(X) = q_1(X)q_2(X)$ and $p_2(X) = q_3(X)q_4(X)$. By definition of the resultant, we have that $R(p_1(X), p_2(X)) = \prod_{i,j}(x_i - x_j')$. Since $p_1(X), p_2(X) \in \mathbb{Q}[X]$, $R(p_1(X), p_2(X)) \in \mathbb{Q}$. By Lemma 2.3.3, $D(p_1p_2) = s^2$ for some $s \in \mathbb{Q}$. Since the roots of each p_j contain (only) a 4-cycle of $\phi(X)$, by Theorem 2.3.4, the trace of the roots of p_j, say z_j, is rational for $j = 1, 2$. Clearly, $u := z_1z_2$ and $v := z_1 + z_2$ are rational. By Lemma 2.3.2, we also have that

$$\begin{aligned}
p_j(X) &= p_{z_j}(X) \\
&= X^4 - z_j X^3 - \frac{z_j^2 + 3z_j + 4}{2z_j} X^2 + \frac{z_j^3 + 2z_j^2 + 5z_j + 8}{4} X \\
&\quad - \frac{z_j^6 + 2z_j^5 + 4z_j^4 + 6z_j^3 - 5z_j^2 - 8z_j - 16}{16z_j^2},
\end{aligned}$$

for $j = 1, 2$. Now we are in the same situation as in the proof of Theorem 2.3.4 (using that $R(p_1(X), p_2(X))$, u and v are rational). Thus, we can use the same argument as in the proof of Theorem 2.3.4 to show that this is impossible. □

The consequence of Theorem 2.3.4 is that we know all 4-periodic points over quadratic fields for $\phi(x) = x^2 + c$, where $c \in \mathbb{Q}$.

Theorem 2.3.6. *Let $\phi(z) = z^2 + c$. Then*

(a) *c and the points of period 4 can be parametrized over $\mathbb{C}$ by the following:*

$$c = \frac{1 - 4t^3 - t^6}{4t^2(t^2 - 1)},$$

$$x_1 = \frac{t^4 - t^2 + \sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)}, x_2 = \frac{1 - t^2 + t\sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)},$$
$$x_3 = \frac{t^4 - t^2 - \sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)}, x_4 = \frac{1 - t^2 - t\sqrt{(t^4 - 1)(t^2 + 2t - 1)}}{2t(t^2 - 1)},$$

where $t = x_1 + x_3$.

(b) *Assume that $c \in \mathbb{Q}$ and x_1, x_2, x_3, x_4 lie in a quadratic field, then $t \in \mathbb{Q}$. Therefore, as t ranges through $\mathbb{Q}$, we obtain all 4-cycles over quadratic fields.*

2.4 Points of Period 6

From Stoll's paper [24], assuming the Birch and Swinnerton-Dyer Conjecture, there are no rational points on $\Phi_6^*(x,c) = 0$ for $c \in \mathbb{Q}$. To be more precise, there are no rational points of primitive period 6 for $\phi(x) = x^2 + c$ where $c \in \mathbb{Q}$. However, there is a quadratic 6-cycle for $c = -\frac{71}{48}$. It is natural to ask if the analog of Theorem 2.3.4 holds; namely is $\overline{x}_4 = x_1$ for period 6? For a point $(x,c) \in X_0(6) : \Phi_6^*(x,c) = 0$, we consider the "trace" of its orbit,

$$x + \phi(x) + \phi^2(x) + \cdots + \phi^5(x,c).$$

The resultant with respect to x of $\Phi_6^*(x,c)$ and $t - (x + \phi(x) + \phi^2(x) + \cdots + \phi^5(x,c))$ is a sixth power; one of its six roots is

$$\begin{aligned}\Psi_6(x,c) =& 256(t^3 + t^2 - t - 1)c^3 + 16(9t^5 + 7t^4 + 10t^3 + 30t^2 - 19t - 37)c^2 \\ &+ 8(3t^7 + t^6 + 2t^5 + 2t^4 - 17t^3 + 69t^2 + 52t - 48)c \\ &+ t^9 - t^8 + 2t^7 + 14t^6 + 49t^5 + 175t^4 + 140t^3 + 196t^2 + 448t.\end{aligned}$$

(This polynomial was already computed by Morton in [13].) Assuming the Birch and Swinnerton-Dyer Conjecture, Stoll [24] proved that there are exactly 10 rational points on $\Psi_6(x,c)$. Only one of them, $(t,c) = (-\frac{7}{2}, -\frac{71}{48})$, can generate a 6-cycle over a quadratic field. If we also assume that $\overline{x}_1 = x_4$ holds for all quadratic 6-cycles (the analogue of Theorem 2.3.4), when $c \in \mathbb{Q}$, then the traces must be rational. Then $\phi(x) = x^2 - \frac{71}{48}$ is the only rational quadratic polynomial (up to linear equivalence) that has a 6-cycle over a quadratic field.

Chapter 3

Periodic Points and Dynamical Units

3.1 Overview

Fix the n^{th} root of unity $\mu = e^{2\pi i/n}$. The cyclotomic units can be constructed using $1 - \mu^j$ for $1 \leq j \leq n-1$. One of our goals in this chapter is to study this theory for the periodic points of a rational function $\phi \in K(z)$, or equivalently of a rational map $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$. In other words, we will study units in the fields generated by the periodic points of ϕ . By analogy with the cyclotomic theory and in recognition of the dynamical study of periodic points of rational maps, we will call the units constructed by periodic points *dynamical units*. Some of these were originally constructed by Narkiewicz [16], then was reformulated and generalized by Morton and Silverman [15].

3.2 Background

We study dynamics of rational maps ϕ over fields K with valuations that have "good reduction." This means that the reduction of ϕ modulo the maximal ideal of the ring of integers of K is a "well-behaved" rational map $\widetilde{\phi}$ over the residue field k of K. Thus, studying the dynamics of $\widetilde{\phi}$ over k allows us to derive information about the dynamics of ϕ over K. We set the following notation:

K a field with normalized discrete valuation $v : K^* \to \mathbb{Z}$

$|\cdot| = c^{-v(x)}$ for some $c > 1$, an absolute value associated to v.

$R = \{\alpha \in K : v(\alpha) \geq 0\}$, the ring of integers of K.

$\mathfrak{p} = \{\alpha \in K : v(\alpha) \geq 1\}$, the maximal ideal of R.

$R^* = \{\alpha \in K : v(\alpha) = 0\}$, the group of units of R.

$k = R/\mathfrak{p}$, the residue field of R.

$\sim$ reduction modulo $\mathfrak{p}$, i.e., $R \to k, a \mapsto \widetilde{a}$.

The following theorem will provide the notion of "good reduction", see [23].

Definition 1. *Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map and write*

$$\phi = [F(X, Y), G(X, Y)]$$

with homogeneous polynomials $F, G \in K[X, Y]$ and gcd$(F, G) = 1$. We say that the pair (F, G) is ***normalized****, or has been written in* ***normalized form****, if $F, G \in R[X, Y]$ and at least one coefficient of F or G is in R^*.*

Equivalently, $\phi = [F, G]$ is normalized if

$$F(X, Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_{d-1}XY^{d-1} + a_dY^d$$

and

$$G(X, Y) = b_0X^d + b_1X^{d-1}Y + \cdots + b_{d-1}XY^{d-1} + b_dY^d$$

satisfy

$$\min\{v(a_0), v(a_1), \ldots, v(a_d), v(b_0), v(b_1), \ldots, v(b_d)\} = 0.$$

Definition 2. *Let* $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ *be a rational map defined over a field* K *with nonarchimedean absolute value* $|\cdot|_v$ *. Write* $\phi = [F, G]$ *using a pair of normalized homogeneous polynomials* $F, G \in R[X, Y]$*. The resultant of* ϕ *is the quantity* $Res(\phi) = Res(F, G)$*.*

Theorem 3.2.1. *[23] Let* $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ *be a rational map defined over* K *and write* $\phi = [F, G]$ *in normalized form. The following are equivalent:*

(a) $deg(\phi) = deg(\widetilde{\phi})$.

(b) *The equation* $\widetilde{F}(X, Y) = \widetilde{G}(X, Y) = 0$ *has no solution* $[\alpha, \beta] \in \mathbb{P}^1(\overline{k})$.

(c) $Res(\phi) \in R^*$.

(d) $Res(F, G) \neq 0$.

Definition 3. *A rational map* $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ *defined over* K *is said to have* ***good reduction (modulo v)*** *if it satisfies any one (hence all) of the conditions of Theorem 3.2.1.*

Since, in general, periodic points might not lie in the base field, one sometimes need to study the points in the extension of the base field. The following theorem enables one to study the extensions of a field with valuation.

Theorem 3.2.2. *[10] Let* K *be a subfield of a field* L*. Then a valuation on* K *has an extension to a valuation on* L*.*

3.3 Periodic Points and Dynamical Units

Recall that the chordal metric on $\mathbb{P}^1(\mathbb{C})$, which we now denote by ρ_∞, is defined by the formula

$$\rho_\infty(P_1, P_2) = \frac{|X_1Y_2 - X_2Y_1|}{\sqrt{|X_1|^2 + |Y_1|^2}\sqrt{|X_2|^2 + |Y_2|^2}}$$

for points $P_1 = [X_1, Y_1]$ and $P_2 = [X_2, Y_2]$ in $\mathbb{P}^1(\mathbb{C})$. In the case of a field K having a nonarchimedean absolute value $|\cdot|_v$, it is convenient to use a metric given by a slightly different formula.

Definition 4. *Let K be a field with a nonarchimedean absolute value $|\cdot|_v$, and let $P_1 = [X_1, Y_1]$ and $P_2 = [X_2, Y_2]$ be points in $\mathbb{P}^1(K)$. The **v-adic chordal metric** on $\mathbb{P}^1(K)$ is*

$$\rho_v(P_1, P_2) = \frac{|X_1Y_2 - X_2Y_1|_v}{\max\{|X_1|_v, |Y_1|_v\} \max\{|X_2|_v, |Y_2|_v\}}.$$

It is clear from the definition that $\rho_v(P_1, P_2)$ is independent of the choice of homogeneous coordinates for P_1 and P_2.

The following proposition will confirm that ρ_v is indeed a metric. In fact, it is an ultrametric, i.e., it satisfies the nonarchimedean triangle inequality.

Proposition 3.3.1. *[23]*

(a) $1 \geq \rho_v(P_1, P_2) \geq 0$ *for all* $P_1, P_2 \in \mathbb{P}^1(K)$.

(b) $\rho_v(P_1, P_2) = 0$ *if and only if* $P_1 = P_2$.

(c) $\rho_v(P_1, P_2) = \rho_v(P_2, P_1)$.

(d) $\rho_v(P_1, P_3) \leq \max\{\rho_v(P_1, P_2), \rho_v(P_2, P_3)\}$.

Lemma 3.3.2. *[23] Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map that has good reduction. Then the map ϕ is everywhere nonexpanding:*

$$\rho_v(\phi(P_1), \phi(P_2)) \leq \rho_v(P_1, P_2)$$

for all $P_1, P_2 \in \mathbb{P}^1(K)$.

As their name suggests, rational maps with good reduction behave well when they are reduced. For the proof of the following theorem see [23].

Theorem 3.3.3. *[23] Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map that has good reduction. Then*

(a) $\widetilde{\phi}(\widetilde{P}) = \widetilde{\phi(P)}$ *for all $P \in \mathbb{P}^1(K)$*

(b) *Let $\psi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be another rational map with good reduction. Then the composition $\phi \circ \psi$ has good reduction, and $\widetilde{\phi \circ \psi} = \widetilde{\phi} \circ \widetilde{\psi}$.*

Proposition 3.3.4. *[23] Let $\phi(z) \in K(z)$ be a rational function of degree $d \geq 2$ with good reduction.*

(a) *Let $P \in \mathbb{P}^1(K)$ be a point of period n for ϕ. Then $\rho_v(\phi^i P, \phi^j P) = \rho_v(\phi^{i+k} P, \phi^{j+k} P)$ for all $i, j, k \in \mathbb{Z}$, where for $i < 0$ we use the periodicity $\phi^n P = P$ to define $\phi^i P$.*

(b) *Let $P \in \mathbb{P}^1(K)$ be a point of exact period n for ϕ. Then $\rho_v(\phi^i P, \phi^j P) = \rho_v(\phi P, P)$ for all $i, j \in \mathbb{Z}$ satisfying $\gcd(i - j, n) = 1$.*

(c) *Let $P_1, P_2 \in \mathbb{P}^1(K)$ be periodic points for ϕ of exact period n_1 and n_2, respectively. Assume that $n_1 \nmid n_2$ and $n_2 \nmid n_1$. Then $\rho_v(P_1, P_2) = 1$.*

Definition 5. *Let $P_1, P_2, P_3, P_4 \in \mathbb{P}^1(K)$, and choose homogeneous coordinates $P_i = [x_i, y_i]$ for each point. The cross-ratio of P_1, P_2, P_3, P_4 is the quantity*

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

Notice that $\kappa(P_1, P_2, P_3, P_4)$ is independent of the choice of homogeneous coordinates for the points.

Remark: There are different definitions for the cross-ratios. However, the given definition seems to suit studying arithmetic dynamics.

Theorem 3.3.5. *[23, 15] Let $\phi \in K(z)$ be a rational map of degree $d \geq 2$ with good reduction. Let $P \in \mathbb{P}^1(K)$ be a periodic point for ϕ of exact period n, and let i and j be integers satisfying*

$$gcd(i, n) = gcd(j - 1, n) = gcd(i - j, n) = 1.$$

Then

$$\kappa(P, \phi(P), \phi^i(P), \phi^j(P)) \in R^*.$$

Theorem 3.3.6. *[23, 15] Let $\phi \in K(z)$ be a rational map of degree $d \geq 2$ with good reduction. Let $n_1, n_2 \in \mathbb{Z}$ be integers with $n_1 \nmid n_2$ and $n_2 \nmid n_1$, let $P_1, P_2 \in \mathbb{P}^1(K)$ be periodic points of exact periods n_1 and n_2, respectively, and write $P_i = [x_i, y_i]$ in normalized form. Then $x_1y_2 - x_2y_1 \in R^*$.*

Remark: The statement of the Theorem 3.3.5 in [23] incorrectly switches i and j. The statement in [15] is correct. Theorem 3.3.6 can be extended to the preperiodic points by the following.

Proposition 3.3.7. *Let $\phi(z) \in K(z)$ be a rational function of degree $d \geq 2$ with good reduction. Let $P_1, P_2 \in \mathbb{P}^1(K)$ be preperiodic points for ϕ of exact periods n_1 and n_2, respectively. Assume that $n_1 \nmid n_2$ and $n_2 \nmid n_1$. Then $\rho_v(P_1, P_2) = 1$.*

Proof. Since P_1, P_2 are preperiodic points, there is $k \in \mathbb{N}$ such that $\phi^k(P_1)$ and $\phi^k(P_2)$ are periodic points of exact periods n_1 and n_2, respectively. By Proposition 3.3.4, $\rho_v(\phi^k(P_1)_1, \phi^k(P_2)) = 1$. By Proposition 3.3.1(a) and Lemma 3.3.2, $\rho_v(P_1, P_2) = 1$. $\square$

Theorem 3.3.8. *Let $\phi(z) \in K(z)$ be rational function of degree $d \geq 2$ with good reduction. Let $n_1, n_2 \in \mathbb{N}$ with $n_1 \nmid n_2$ and $n_2 \nmid n_1$, let $P_1, P_2 \in \mathbb{P}^1(K)$ be preperiodic points for ϕ of exact periods n_1 and n_2, respectively, and write $P_i = [x_i, y_i]$ in normalized form. Then*

$$x_1y_2 - x_2y_1 \in R^*.$$

Moreover, if ϕ is even, then $x_1y_2 \pm x_2y_1 \in R^*$.

Proof. Since P_i are in normalized form, the chordal metric is given by

$$\rho_v(P_1, P_2) = \mid x_1y_2 - x_2y_1 \mid_v .$$

The assumptions on n_1 and n_2 and Proposition 3.3.7 imply that $\rho_v(P_1, P_2) = 1$, and hence $x_1y_2 - x_2y_1$ is a unit. Now assume that ϕ is even. Thus, $-x_2$ is also a preperiodic point. Then $x_1y_2 \pm x_2y_1 \in R^*$. $\square$

Morton and Silverman show in [15] that we can use periodic points of rational functions to produce units over fields with valuations. We will consider the converse problems of the results in [15]. To be more precise, we consider the following question:

What are the forms that we can use to produce units from periodic points of rational functions over fields with valuations?

We will prove that, under certain conditions, the form that can be used to generate the units is unique.

Proposition 3.3.9. *Let K be a number field and let T be a finite set of places of K that includes the archimedean places. Let $\widetilde{T}$ be the set of places of $\overline{\mathbb{Q}}$ lying over the places of T. Let $a, b \in K$. Suppose p is a prime number and ζ_p is a primitive pth root of unity such that*

$$a^{p^m}\zeta_p + b^{p^m}$$

is a $\widetilde{T}$-unit of $K(\zeta_p)$ for infinitely many positive integers m. Then each of a, b is a T-unit or 0. If $ab \neq 0$ then a/b is a root of unity.

Proof. For each m as in the statement, write

$$u_m^{-1}a^{p^m}\zeta_p + u_m^{-1}b^{p^m} = 1,$$

where u_m is a T-unit. Let S be the set of primes occuring in the factorizations of a and b plus the places in T. The S-unit theorem (applied to $K(\zeta_p)$) says that $u+v=1$ has only finitely many solutions in S-units u and v (see [11, 22]). Therefore, there are indices $m_1 \neq m_2$ such that

$$u_{m_1}^{-1}a^{p^{m_1}} = u_{m_2}^{-1}a^{p^{m_2}}.$$

This implies that a power of a is a T-unit, hence a is a T-unit. Similarly, b is a T-unit.

Let T' be the set of places of $K(\zeta_p)$ above T. The group of T'-units of $K(\zeta_p)$ is finitely generated, so there are finitely many cosets mod p-th powers. Write each u_m in the form wv_m^p with w from a finite set of representatives mod pth powers. Some w, call it w_0, occurs for infinitely many m. Therefore, for these m,

$$w_0^{-1}(a^{p^{m-1}}v_m^{-1})^p\zeta_p + w_0^{-1}(b^{p^{m-1}}v_m^{-1})^p = 1.$$

The S-unit theorem implies that there are indices m' and m'' such that

$$a^{p^{m'-1}}v_{m'}^{-1} = a^{p^{m''-1}}v_{m''}^{-1}$$

and

$$b^{p^{m'-1}}v_{m'}^{-1} = b^{p^{m''-1}}v_{m''}^{-1}.$$

The ratio of these two relations (if $ab \neq 0$) yields

$$(a/b)^{p^{m'-1}-p^{m''-1}} = 1.$$

Therefore, if $ab \neq 0$ then a/b is a root of unity. $\square$

We can now prove a converse to Theorem 3.3.6.

Theorem 3.3.10. *Let K be number field and let T be finite set of places of K that includes the archimedean places. Let $\widetilde{T}$ be a set of places of $\overline{\mathbb{Q}}$ lying above the places in T. Suppose $a, b, c, d \in K$ are such that*

$$B([x_1, y_1], [x_2, y_2]) = ax_1x_2 + bx_1y_2 + cx_2y_1 + dx_2y_2$$

is a $\widetilde{T}$-unit whenever ϕ is a rational function of degree at least 2 defined over K with everywhere good reduction, $[x_1, y_1] \in \mathbb{P}^1(\overline{\mathbb{Q}})$ is a normalized point of order 2 and $[x_2, y_2] \in \mathbb{P}^1(\overline{\mathbb{Q}})$ is a normalized point of order 3 for ϕ. Then $a = 0 = d$ and $b = -c$. Moreover, b and c are T-units.

Proof. Let $p \equiv 1 \pmod 3$ be prime. Let $m \geq 1$ and let n have order 6 in $(\mathbb{Z}/p^{m+1}\mathbb{Z})^\times$. Let k be an integer and let $\phi(x) = k + (x-k)^{-n}$. Then $[x_1, y_1] = [k, 1]$ and $[1, 0]$ have order 2 for ϕ and $[k+\zeta, 1]$ has order 3, where ζ is any primitive p^{m+1}st root of unity.

We have that

$$B([1,0],[k+\zeta,1]) = a\zeta + (ak+b)$$

is a $\widetilde{T}$-unit in $K(\zeta)$ for each primitive p^{m+1}-th root of unity ζ. Fix one such ζ.

The product

$$u_m = \prod_{j=1}^{p^m} (a\zeta^{1+jp} + (ak+b)) = a^{p^m}\zeta_p + (ak+b)^{p^m}$$

is a $\widetilde{T}$-unit (where $\zeta_p = \zeta^{p^m}$). If $a \neq 0$ then $ak + b \neq 0$ for sufficiently large k. The proposition implies that $(ak+b)/a$ is a root of unity for large k. Absolute values show that this is impossible. Therefore $a = 0$. Therefore, b is a T-unit.

Now conjugate ϕ by $(1/x)$ to obtain

$$\psi(x) = \frac{(1-kx)^n}{k(1-kx)^n + x^n}.$$

Then $[x_1, y_1] = [1, k]$ and $[0, 1]$ have order 2 for ψ and $[1, k+\zeta]$ has order 3, where ζ is any primitive p^{m+1}st root of unity. We find that $d = 0$ and c is a T-unit.

Now compute

$$B([k,1],[k+\zeta,1]) = (b+c)k + c\zeta.$$

If $b+c \neq 0$, we find that $(b+c)k/c$ is a root of unity for all $k > 0$. This is impossible. Therefore, $b = -c$. $\square$

3.4 Bounds for Period Lengths

Morton and Silverman show in [14] that a rational periodic point of a rational map with good reduction at 2 and 3 has period dividing 24. In this section we will demonstrate a simple form of the boundedness of preperiodic points.

Definition 6. *Let K be a number field. Let $\phi(z) \in K(z)$. We say that $\phi(z)$ has **good reduction everywhere**, if $\phi(z)$ has good reduction modulo v, for all non-archimedean valuation v defined over K.*

Theorem 3.4.1. *Let $\phi \in \mathbb{Q}(z)$ with good reduction everywhere (outside ∞). Assume that ϕ has an n-cycle consisting of rational integers. Then $n \leqslant 2$.*

Proof. Assume to the contrary that there is an integral n-cycle and $n \geq 3$. Let P be an integral point in the cycle. By Proposition 3.3.4(b), $\rho_v(\phi^{n-1}P, P) = \rho_v(\phi P, P)$. Since P is a point of exact period $n \geq 3$, $P, \phi P$ and $\phi^{n-1}P$ are all different. Write $\phi^i P = [x_i, y_i]$ and $\phi^j P = [x_j, y_j]$. Since $\phi^k P \in \mathbb{Z}$ for all $k \in \mathbb{Z}$, we may take $y_i = y_j = 1$. Thus,

$$\rho_v(\phi^i P, \phi^j P) = \frac{| \, x_i y_j - x_j y_i \, |_v}{\max\{| \, x_i \, |_v, | \, y_i \, |_v\} \max\{| \, x_j \, |_v, | \, y_j \, |_v\}} = |\phi^i P - \phi^j P|_v,$$

for each valuation v over $\mathbb{Q}$. By Proposition 3.3.4(a), $\rho_v(\phi P, P) = \rho_v(\phi^i P, \phi^{i-1}P)$ for all $i \in \mathbb{Z}$. Thus, $\rho_v(\phi^{n-1}P, P) = \rho_v(\phi P, P) = \rho_v(\phi^i P, \phi^{i-1}P)$ for all $i \in \mathbb{Z}$. Therefore,

$$|\phi^{n-1}P - P|_v = |\phi P - P|_v = |\phi^i P - \phi^{i-1}P|_v$$

for all non-archimedean v. Therefore, for the usual absolute value,

$$|\phi^{n-1}P - P| = |\phi P - P| = |\phi^i P - \phi^{i-1}P|.$$

Without loss of generality, assume $\phi^{n-1}P < P$. Thus,

$$\phi^{n-1}P < P < \phi P < \phi^2 P < ... < \phi^{n-2}P < \phi^{n-1}P,$$

a contradiction. Therefore, $n \leq 2$. $\square$

To improve the bound of [14], we need some identities relating the Fibonacci numbers to the cross ratio. Recall that the Fibonacci numbers are the sequence of numbers $\{F_n\}_{n=1}^{\infty}$ defined by the linear recurrence equation

$$F_n = F_{n-1} + F_{n-2}$$

with $F_1 = F_2 = 1$.

Theorem 3.4.2. *(a) (Catalan's identity [4] p. 402)*

$$F_n^2 - F_{n+r}F_{n-r} = (-1)^{n-r}F_r^2,$$

(b) (d'Ocagne's identity [5])

$$F_m F_{n+1} - F_n F_{m+1} = (-1)^n F_{m-n}.$$

Theorem 3.4.3. *Let $c \in \mathbb{C}$. Let $K_1(c) = 0$, $K_2(c) = 1$, $K_3(c) = c$ and*

$$K_n(c) = \frac{cF_{n-1}}{F_{n-2} + cF_{n-3}}$$

for $n \geq 4$. Then

$$\kappa(K_n(c), K_{n+1}(c), K_{n+2}(c), K_{n+3}(c)) = -1$$

for all $n \in \mathbb{N}$ where $K(a_1, a_2, a_3, a_4)$ is the cross ratio of (a_1, a_2, a_3, a_4) (defined in Section 3.3).

Proof. For $n \leq 3$ we can compute directly that

$$\kappa(K_n(c), K_{n+1}(c), K_{n+2}(c), K_{n+3}(c)) = -1.$$

Let $n \geq 4$. Then

$$\kappa(K_n(c), K_{n+1}(c), K_{n+2}(c), K_{n+3}(c)) = \frac{A \times B}{C \times D},$$

where

$$A = -F_nF_{n+1} - cF_n^2 + F_{n+2}F_{n-1} + F_{n+2}cF_{n-2}$$

$$B = -F_{n-1}F_n - cF_{n-1}^2 + F_{n+1}F_{n-2} + F_{n+1}cF_{n-3}$$

$$C = -F_{n+1}^2 - F_{n+1}cF_n + F_{n+2}F_n + F_{n+2}cF_{n-1}$$

$$D = -F_{n-1}^2 - F_{n-1}cF_{n-2} + F_nF_{n-2} + F_ncF_{n-3}.$$

Applying Catalan's and d'Ocagne's identities to numerators and denominators, we have

$$\kappa(K_n, K_{n+1}, K_{n+2}, K_{n+3}) = \frac{(-1)^{n-2}(1-c)(-1)^{n-3}(1-c)}{(-1)^{n-1}(1-c)(-1)^{n-3}(1-c)} = -1.$$

$\square$

Theorem 3.4.4. *Let $\phi \in \mathbb{Q}(z)$ with good reduction everywhere (outside ∞). Assume that ϕ has a rational n-cycle. Then $n \mid 6$.*

Proof. Let $P \in \mathbb{Q}$ be a primitive n-periodic point of ϕ. By Theorem 3.3.5, $\kappa(P, \phi P, \phi^i P, \phi^j P)$ is a local unit for each v of good reduction, when $\gcd(i, n) =$

$\gcd(j-1,n)=\gcd(i-j,n)=1$. Since ϕ has good reduction everywhere, $\kappa(P,\phi P,\phi^i P,\phi^j P)=\pm 1$. However, from computation,

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

for all $P_1,P_2,P_3,P_4\in\mathbb{P}^1$. Since $\kappa(P_1,P_2,P_4,P_3)\neq 0$, this implies that $\kappa(P,\phi P,\phi^2 P,\phi^3 P)=-1$.

Note that κ is invariant under linear transformations $f(x)=ax+b\in K(x)$. Without loss of generality, we can assume that $P=0,\phi P=1,\phi^2 P=c$ and $\phi^3 P=d$, for some $c,d\in\mathbb{Q}$. We have that $\kappa(0,1,c,d)=-1$. Thus, $d=\frac{2c}{c+1}$. In general, if $\kappa(a_1,a_2,a_3,a_4)=-1$, then

$$a_4=\frac{a_1a_2-2a_3a_2+a_1a_3}{2a_1-a_3-a_2}.$$

That means the sequence of periodic points is uniquely determined by the first 3 iterations.

Case 1 $n=4$.

Let P be a point in a rational cycle of primitive period 4. Choose $i=3$ and $j=2$. We have $\kappa(P,\phi P,\phi^3 P,\phi^2 P)+\kappa(P,\phi P,\phi^2 P,\phi^3 P)=1$. Since $\kappa(P,\phi P,\phi^3 P,\phi^2 P)=-1$ (by Theorem 3.3.5), $\kappa(P,\phi P,\phi^2 P,\phi^3 P)=2$. However,

$$\mid\kappa(P,\phi P,\phi^2 P,\phi^3 P)\mid_2=\frac{\rho_2(P,\phi^2 P)\rho_2(\phi P,\phi^3 P)}{\rho_2(P,\phi P)\rho_2(\phi^2 P,\phi^3 P)}=\left(\frac{\rho_2(P,\phi^2 P)}{\rho_2(P,\phi P)}\right)^2.$$

This is a contradiction, since $\frac{\rho_2(P,\phi^2 P)}{\rho_2(P,\phi P)}\in\mathbb{Q}$ and $2\neq r^2$ for all $r\in\mathbb{Q}$.

Case 2 $n\geq 5$ and $n\neq 6$.

Write $n=2^k s$, where $\gcd(2,s)=1$.

If $k\geq 2$, we can consider the rational cycle of primitive 4-period of $\psi=\phi^{n/4}$ which we have proved impossible.

If $k \leq 1$, then n is odd, or $\frac{n}{2}$ is odd. Thus, we can consider $\psi = \phi^2$ if necessary. Without loss of generality, assume n is odd. Choose $i = 2$ and $j = 3$. Let $P = 0, \phi P = 1, \phi^2 P = c$. Then $\phi^3 P = \dfrac{2c}{c+1} = K_4(c)$. Since the sequence of periodic points is uniquely determined by the first 3 iterations, $\phi^{n-1}P = K_n(c)$ for all $n \in \mathbb{N}$. However, $K_{n+3}(c) = \dfrac{cF_{n+2}}{F_{n+1} + cF_n} \neq 0$, for all $n \in \mathbb{N}$. Thus, $\phi^n P \neq 0$ for all $n \in \mathbb{N}$. This contradicts to the periodicity of P. $\square$

We can also prove Theorem 3.4.4 without using Fibonacci identities.

Proof. From the proof above we use that the sequence of periodic points is uniquely determined by the first 3 iterations.

Let P be a rational point of primitive period n. There is at most one positive integer $j < n$ such that $\kappa(P, \phi P, \phi^2 P, \phi^j P) = -1$. We will use this to give a proof without the Fibonacci sequence.

Case 1 $n = 4$.

Use the same method as the proof above.

Case 2 $n = 5k$.

If $n = 5$, we have

$$\kappa(P, \phi P, \phi^2 P, \phi^3 P) = -1 = \kappa(P, \phi P, \phi^2 P, \phi^4 P).$$

This yields $\phi^3 P = \phi^4 P$, contradiction. If $n = 5k$ and $k > 1$, we can consider $\psi = \phi^k$.

Case 3 $n > 6$.

Write $n = 2^k s$, where $\gcd(2, s) = 1 = \gcd(5, s)$.

If $k \geq 2$, we can consider the rational cycle of primitive period 4 of $\psi = \phi^{n/4}$ which we have proved impossible.

If $k \leq 1$, then n is odd, or $\frac{n}{2}$ is odd. Thus, we can consider $\psi = \phi^2$ if necessary. Without loss of generality, assume n is odd. We choose $i = 2$, $j_1 = 3$ and $j_2 = 6$. Since the sequence of periodic points is uniquely determined by the first 3 iterations, $\phi^3 P = \phi^6 P$, contradiction. $\square$

Remark: We don't know if $n = 6$ is impossible.

Bibliography

[1] T. Bousch. *Sur Quelques Problèmes de Dynamique Holomorphe.* PhD thesis, Universite de Paris-Sud, Centre d′Orsay, 1992.

[2] J. K. Canci. Finite orbit for rational functions. *Indag. Mathem., N.S.* **18**(2), 203-214, 2007.

[3] J. E. Cremona. *Algorithms for Modular Elliptic Curves, Online Edition.* http://www.warwick.ac.uk/ masgaj/book/fulltext/index.html, 2005.

[4] L. E. Dickson. *History of the Theory of Numbers* Vol. 1. Chelsea Publishing Company, 1952.

[5] M. Edson and O. A. Yayenie. New generalization of Fibonacci sequence and extended Binet's formula. *Integers.* **9**, 639-654, 2009.

[6] T. Erkama. Periodic orbits of quadratic polynomials. *Bull. London Math. Soc.* **38**, 804-814, 2006.

[7] N. Fakhruddin. Questions on self maps of algebraic varieties. *J. Ramanujan Math. Soc.* **18**(2), 109-122, 2003.

[8] E. V. Flynn, B. Poonen and E. F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Math. J.* **90**(3), 435-463, 1997.

[9] B. Hutz. Dynatomic cycles for morphisms of projective varieties. *New York J. Math.* **16**, 125-159, 2010.

[10] S. Lang. *Algebra, Third Edition.* Springer, 2002.

[11] K. Mahler. On algebraic relations between two units of an algebraic field, Algèbre et Théorie des Nombres. *Colloques Internationaux du Centre National de la Recherche Scientifique.* **24**, 47-55, 1950.

[12] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.* **124**(1-3), 437-449, 1996.

[13] P. Morton. Arithmetic properties of periodic points of quadratic maps II. *Acta Arith.* **87(2)**, 89-102, 1998.

[14] P. Morton and J. H. Silverman. Rational periodic points of rational functions. *internat. Math. Res. Notices.* **2**, 97-110, 1994.

[15] P. Morton and J. H. Silverman. Periodic points, multiplicity and dynamical units. *J. Reine Angew. Math.* **461**, 81-122, 1995.

[16] W. Narkiewicz. Polynomial cycles in algebraic number fields. *Colloq. Math.* **58**(1), 151-155, 1989.

[17] E. Netto. *Vorlesungen über Algebra II.* Teubner, 222-227, 1900.

[18] D. G. Northcott. Periodic points on an algebraic variety. *Ann. of Math.* **2**(51), 167-177, 1950.

[19] B. Poonen. The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture. Math. Z. **228**(1), 11-29, 1998.

[20] V. V. Prasolov. *Polynomials.* Springer, 2010.

[21] P. Russo and R. Walde. Rational periodic points of the quadratic function $\mathbb{Q}_c(x) = x^2 + c$. *Amer. Math. Monthly.* **101**, 318-331, 1994.

[22] C. L. Siegel. Approximation algebraischer Zahlen. *Math. Z.* **10**, 173-213, 1921.

[23] J. H. Silverman. *The Arithmetic of Dynamical Systems.* Springer, 2007.

[24] M. Stoll. Rational 6-cycles under iteration of quadratic polynomials. *LMS J. Comput. Math.* **11**, 367-380, 2008.

[25] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition.* Chapman and Hall/CRC, 2008.