WELL-BEHAVING DYNAMICS OVER $\mathbb{Q}_p$

YANNIS WU-YIP

Abstract. This paper aims to provide an introduction to the p-adic numbers and an overview of the dynamics of well-behaving rational maps over a p-adic field, culminating in the analysis of an extended example. We only assume familiarity of algebra and elementary number theory.

Contents

1. Introduction

Like complex dynamics, the overarching goal in arithmetic dynamics is to analyze and understand the iteration of self-maps but on a p-adic field such as $\mathbb{Q}_p$ rather than the complex plane $\mathbb{C}$. Though there are many options of self-maps, polynomial and rational maps are especially interesting since they are the simplest kinds of maps. Properties of potential interest include whether an orbit $\{z, f(z), f(f(z)), \dots\}$ of a map f is finite over a given field and whether there exist fixed points for a map f.

To introduce some notation, a point P is called *periodic* if $f^n(P) = P$ for some $n \geq 1$. Moreover, a point P is called *pre-periodic* if $f^m(P)$ is periodic for some $m \geq 1$, that is $f^m(P) = f^n(P)$ for some $n > m$. Thus we can also ask what do the sets $\mathrm{Per}(f)$ and $\mathrm{PrePer}(f)$ look like for f a polynomial or rational map. In fact there is a conjecture of Morton-Silverman regarding the size of the set of pre-periodic points of a polynomial f over a number field K, such as $\mathbb{Q}$.

Conjecture 1.1 (Uniform Boundedness Conjecture (UBC))**.** *Let K be a number field and $\phi : \mathbb{P}^N(K) \to \mathbb{P}^N(K)$ be any finite morphism of degree d. Then, the number of pre-periodic points of ϕ over K is bounded by a constant:*

$$\#PrePer(\phi, K) \leq \mathcal{C}(d, N, \deg(K/\mathbb{Q}))$$

The Uniform Boundedness Conjecture has a few corollaries. One of which is Mazur's Theorem on torsion points of elliptic curves.

Theorem 1.2 (Mazur's Theorem)**.** *For an elliptic curve E over a number field K, the number of torsion points $\#(E_{tors}(K))$ is bounded by a constant C, independent of the elliptic curve and dependent only on the number field K.*

In order to understand dynamics of polynomials and rational maps on $\mathbb{Q}$, we first look to reduce to simpler objects, namely polynomials and rational maps on $\mathbb{Q}_p$. In particular, we will be focused on good-reducing maps, i.e. maps that have the same degree after reduction modulo p. In fact, we are able to classify the forms of the period of a good-reducing rational map on $\mathbb{Q}$. To do so, we will first introduce a metric on $\mathbb{P}^1(K)$, where K is a non-archimedean field, which will provide valuable insight about the reduction process as well as dynamical properties of a map. We then formalize reduction modulo p and present the resultant as a tool to determine when a map has good reduction. Finally, we will discuss known results regarding periodic points of good-reducing rational maps.

In order to discuss such dynamics, we will first provide a short review of the terminology of periodic points. Then, to discuss such dynamics in a number theoretic setting, we will, of course, need to introduce the p-adic numbers.

1.1. **Brief Review of Periodic Points.** Let K be a field with absolute value $|\cdot|$ and let $\phi(z) \in K(z)$ be a rational map. Recall that $\alpha \in \mathbb{P}^1(K)$ has *period* n if n is the smallest value of k such that $\phi^k(\alpha) = \alpha$. Then we can define the *multiplier of* ϕ

$$\lambda_\alpha(\phi) := (\phi^n)'(\alpha) = \prod_{k=0}^{n-1} \phi'(\phi^k(\alpha))$$

The absolute value of $\lambda_\alpha(\phi)$ somewhat characterizes the behavior of ϕ in a small neighborhood around α. If $|\lambda_\alpha(\phi)| < 1$, α is called *attracting*; in particular, if $\lambda_\alpha(\phi) = 0$, α is called *super-attracting*. On the other hand, if $|\lambda_\alpha(\phi)| > 1$, α is called *repelling*. Neutral periodic points, ones that have $|\lambda_\alpha(\phi)| = 1$, are split into *rationally neutral periodic points*, whose multipliers are a root of unity, and those whose multipliers are not a root of unity are called *irrationally neutral periodic points*.

1.2. **The p-adic Numbers.** Just as the real numbers $\mathbb{R}$ is the completion of the rational numbers $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|$, the p-adic numbers $\mathbb{Q}_p$ is the completion of the rational numbers with respect to the p-adic absolute value $|\cdot|_p$. To discuss the p-adics, we first recall the definition of an absolute value:

Definition 1.3. An *absolute value* on a field K is a function $|\cdot| : K \to \mathbb{R}$ such that for all $x, y \in K$

(a) $|x| \geq 0$
(b) $|x| = 0$ iff $x = 0$
(c) $|xy| = |x||y|$
(d) $|x + y| \leq |x| + |y|$ (Triangle Inequality)

Example 1.4. The most familiar example of an absolute value is the usual absolute value on $\mathbb{Q}$, that is

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Besides the usual absolute value on $\mathbb{Q}$ there are other absolute values, such as the discrete absolute value, which is as follows:

$$|x| = \begin{cases} 1 & \text{if } x \neq 0 \\ 0 & \text{if } x = 0 \end{cases}$$

To define the p-adic absolute value, we must first define the p-adic valuation of a rational number.

Definition 1.5. Let $x \in \mathbb{Q}$ be a rational number such that $x = p^n \frac{a}{b}$ for some coprime $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 0}$. Then the *p-adic valuation of* x, denoted $v_p(x)$, is n. That is, $v_p(x)$ is the multiplicity of p in the numerator minus the multiplicity of p in the denominator. Additionally, as convention, we take $v_p(0) = \infty$.

Note that the p-adic valuation is an example of a *discrete valuation*. That is, for $v : K^\times \to \mathbb{R}$ a valuation, $v(K^\times)$ is a discrete subgroup of $\mathbb{R}$. Moreover, its *normalized valuation* (denoted ord_v) is a constant multiple of v such that $\text{ord}_v(K^\times) = \mathbb{Z}$.

We can see that the p-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ has the following properties for all $x, y \in \mathbb{Q}$:

(a) $v_p(x) = \infty$ iff $x = 0$
(b) $v_p(xy) = v_p(x) + v_p(y)$
(c) $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$

Definition 1.6. For $x \in \mathbb{Q}$, we define the *p-adic absolute value* $|x|_p = p^{-v_p(x)}$.

Thus the following properties follow for all $x, y \in \mathbb{Q}$:

(a) $|x|_p \geq 0$
(b) $|x|_p = 0$ iff $x = 0$
(c) $|xy|_p = |x|_p \cdot |y|_p$
(d) $|x + y|_p \leq \max\{|x|_p, |y|_p\}$

Observe that these properties for $|\cdot|_p$ are similar to those in Definition 1.3, with the exception of (d). In fact, the p-adic absolute value is an example of a *non-archimedean absolute value*, that is, an absolute value such that $|x + y| \leq \max\{|x|, |y|\}$ (also called the *ultrametric inequality*), which is a stronger property than that of the triangle inequality required for an absolute value (Definition 1.3). Now we will prove the equality condition for the ultrametric inequality.

Proposition 1.7. *Let $|\cdot|_v$ be a non-archimedean absolute value on a field K with $\alpha, \beta \in K$. If $|\alpha|_v \neq |\beta|_v$, then $|\alpha + \beta|_v = \max\{|\alpha|_v, |\beta|_v\}$.*

Proof. Without loss of generality, suppose $|\alpha|_v > |\beta|_v$. First observe that from (d) in Definition 1.6, we have that $|\alpha + \beta|_v \leq \max\{|\alpha|_v, |\beta|_v\} = |\alpha|_v$. To prove opposing inequality, we note that since $|\alpha|_v$ is strictly greater than $|\beta|_v$, so we have that $|\beta|_v < |\alpha|_v = |(\alpha + \beta) - \beta|_v \leq \max\{|\alpha + \beta|_v, |\beta|_v\} = |\alpha + \beta|_v$. Thus, $|\alpha|_v \leq |\alpha + \beta|_v$, as required. □

Moreover, a theorem by Ostrowski classifies absolute values on $\mathbb{Q}$:

Theorem 1.8 (Ostrowski's Theorem)**.** *Up to equivalence, the only non-trivial absolute values on $\mathbb{Q}$ are the (usual) real absolute value $|\cdot|_\infty$ and the p-adic absolute value $|\cdot|_p$, for some prime p.*

Now, analogous to the construction of the real numbers, we can construct the p-adic numbers.

Definition 1.9. The *p-adic numbers* $\mathbb{Q}_p$ is defined as the completion of the rational numbers $\mathbb{Q}$ with the respect to the p-adic absolute value $|\cdot|_p$.

Similarly to how any real number has a decimal expansion, we have the following proposition for the p-adic numbers.

Proposition 1.10. *Let $x \in \mathbb{Q}_p$ be a p-adic number. Then x has a unique p-adic expansion as*

$$x = \sum_{i=k}^{\infty} a_i p^i$$

where $a_i \in \{0, 1, \ldots, p-1\}$ and $k \in \mathbb{Z}$ possibly negative.

Since $\left|p^k\right|_p = \frac{1}{p^k}$ and there are only finitely many negative k, the sequence $\{p^k\}$ converges to 0 with respect to the p-adic absolute value. In particular, unlike the real numbers, where we have examples such as $0.999\cdots = 1$, each p-adic expansion is unique.

2. Projective Space over a Non-Archimedean Field

From this section onward, we begin our inquiry about the dynamics of local fields of well-behaving polynomials and rational functions over a field K with some non-archimedean (v-adic) absolute value $|\cdot|_v$. Though the statements and proofs will be done using $|\cdot|_v$, all of our examples will be using the p-adic absolute value $|\cdot|_p$.

In this section, we introduce the v-adic chordal metric, which is analogous to the usual chordal metric ρ_∞ on $\mathbb{P}^1(\mathbb{C})$:

$$\rho_\infty(P, Q) = \frac{|P_1 Q_2 - P_2 Q_1|}{\sqrt{|P_1|^2 + |P_2|^2} \cdot \sqrt{|Q_1|^2 + |Q_2|^2}},$$

where $P = [P_1, P_2]$ and $Q = [Q_1, Q_2]$ are points in $\mathbb{P}^1(\mathbb{C})$.

Definition 2.1. For K a field with non-archimedean absolute value $|\cdot|_v$, the *v-adic chordal metric on* $\mathbb{P}(K)$ is

$$\rho_v(P, Q) = \frac{|P_1 Q_2 - P_2 Q_1|_v}{\max\{|P_1|_v, |P_2|_v\} \cdot \max\{|Q_1|_v, |Q_2|_v\}},$$

where $P = [P_1, P_2]$ and $Q = [Q_1, Q_2]$ are points in $\mathbb{P}^1(K)$.

The proof of the following proposition can be found on pages 45-47 of [3].

Proposition 2.2. *The v-adic chordal metric is indeed ultrametric, i.e. it has the following properties:*

(a) $0 \leq \rho_v(P, Q) \leq 1$
(b) $\rho_v(P, Q) = 0$ *iff* $P = Q$
(c) $\rho_v(P, Q) = \rho_v(Q, P)$
(d) $\rho_v(P, R) \leq \max\{\rho_v(P, Q), \rho_v(Q, R)\}$

The following fact that elements of $PGL_2(R)$ preserve v-adic chordal distance will prove to be very useful in the next section.

Lemma 2.3. *Let K be a field with non-archimedean absolute value $|\cdot|_v$ and let $R = \{\alpha \in K : |\alpha|_v \leq 1\}$ be the ring of integers in K. Let $f \in PGL_2(R)$. I.e., let $f : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a linear fractional transformation of form*

$$f([X, Y]) = \frac{aX + bY}{cX + dY} = [aX + bY, cX + dY]$$

with $a, b, c, d \in R$ and $ad - bc \in R^\times$ (that is $|ad - bc|_v = 1$).

Then, $\rho_v(f(P), f(Q)) = \rho_v(P, Q)$ for all $P, Q \in \mathbb{P}^1(K)$. That is, f preserves the v-adic chordal distance.

Proof. Write each point $P = [P_1, P_2]$ and $Q = [Q_1, Q_2]$ so that $P_i, Q_i \in R$ and at least one coordinate of each point in $R^\times$. Then $\max\{|P_1|_v, |P_2|_v\} = 1$ and $\max\{|Q_1|_v, |Q_2|_v\} = 1$, so $\rho_v(P, Q) = |P_1Q_2 - P_2Q_1|_v$. Algebraic manipulation gives us

$$\begin{aligned}(ad - bc)P_1 &= d(aP_1 + bP_2) - b(cP_1 + dP_2)\\ -(ad - bc)P_2 &= c(aP_1 + bP_2) - a(cP_1 + dP_2)\end{aligned}$$

and similarly for Q_1 and Q_2.

Since $\max\{|P_1|_v, |P_2|_v\} = 1$ and $|ad - bc|_v = 1$, it follows from the above equations that $\max\{|aP_1 + bP_2|_v, |cP_1 + dP_2|_v\} = 1$, and similarly for Q. Using the fact that $|ad - bc|_v = 1$ again, it follows that

$$\begin{aligned}\rho_v(f(P), f(Q)) &= |(aP_1 + bP_2)(cQ_1 + dQ_2) - (aQ_1 + bQ_2)(cP_1 + dP_2)|_v\\ &= |(ad - bc)(P_1Q_2 - P_2Q_1)|_v\\ &= \rho_v(P, Q)\end{aligned}$$

as required. □

3. Reduction Modulo $\mathfrak{p}$

When studying an object – in this case a rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ – it is often useful to first analyze its reduction modulo a prime, then lift information about its reduction back for global information. As we will see in the later examples, information gathered from many reductions, each with a distinct prime, can allow us to deduce the behavior of ϕ on $\mathbb{Q}$.

To begin, we will use the following notation:

Definition 3.1. Let K be a field with normalized discrete valuation $v : K^\times \to \mathbb{Z}$ and $|\cdot|_v = c^{-v(x)}$ for some $c > 1$, a non-archimedean absolute value associated with v. We also define the following sets:

$$\begin{aligned}R &= \{\alpha \in K : v(\alpha) \geq 0\} = \{\alpha \in K : |\alpha|_v \leq 1\} && \text{Ring of integers of } K\\ \mathfrak{p} &= \{\alpha \in K : v(\alpha) > 0\} = \{\alpha \in K : |\alpha|_v < 1\} && \text{Maximal ideal of } R\\ R^\times &= \{\alpha \in K : v(\alpha) = 0\} = \{\alpha \in K : |\alpha|_v = 1\} && \text{Group of units of } R\\ k &= R/\mathfrak{p} && \text{Residue field of R}\end{aligned}$$

We will also use $\widetilde{\cdot}$ to denote reduction modulo $\mathfrak{p}$, i.e. the map $R \to k$.

First, how do we reduce points modulo $\mathfrak{p}$? Let $P = [x_0, x_1, \ldots, x_N] \in \mathbb{P}^N(K)$ be a point such that there exist some $x_i \notin R$. Thus we cannot reduce immediately. But since $P = [x_0, x_1, \ldots, x_N]$ is homogeneous, we can rescale so that $P = [cx_0, cx_1, \ldots, cx_N]$, where $c \in K^\times$ is sufficiently divisible by $\mathfrak{p}$, so that $cx_i \in R$

for every $1 \leq i \leq N$. However, c must not be overly divisible by $\mathfrak{p}$, otherwise $cx_i \in \mathfrak{p}$ for every i and upon reduction modulo $\mathfrak{p}$, we would have $[0, 0, \ldots, 0] \notin \mathbb{P}^N(k)$.

But how do we formalize this? We want to "clear the denominators" of x_i as efficiently as possible: Choose $\alpha \in K^\times$ such that

$$v(\alpha) = \min\{v(x_0), v(x_1), \ldots, v(x_N)\}.$$

For example, let $\alpha = x_i$ of minimum valuation. Then, $\alpha^{-1}x_j \in R$ for $1 \leq j \leq N$ and we have $P = [\alpha^{-1}x_0, \alpha^{-1}x_1, \ldots, \alpha^{-1}x_N]$, which can be reduced modulo $\mathfrak{p}$.

Since $\alpha = x_i$ of minimal valuation, it follows that $\alpha^{-1}x_i$ is a unit and thus $\widetilde{\alpha^{-1}x_i} \neq 0$. This allows us to make the following definition:

Definition 3.2. For a point $P = [x_0, x_1, \ldots, x_N] \in \mathbb{P}^N(K)$, the *reduction of P modulo $\mathfrak{p}$* is

$$\widetilde{P} = [\widetilde{\alpha^{-1}x_0}, \widetilde{\alpha^{-1}x_1}, \ldots, \widetilde{\alpha^{-1}x_N}] \in \mathbb{P}^N(k)$$

where α is chosen as described above. Moreover, we say P is written in *normalized coordinates* if

$$\min\{v(x_0), v(x_1), \ldots, v(x_N)\} = 0.$$

In such a case, $\widetilde{P} = [\widetilde{x_0}, \widetilde{x_1}, \ldots, \widetilde{x_N}]$.

Next we will show that this reduction of P using α is in fact well-defined.

Proposition 3.3. *Let $P = [x_0, \ldots, x_N] \in \mathbb{P}^N(K)$. Then the reduction $\widetilde{P}$ is independent of the choice of α such that $v(\alpha) = \min\{v(x_0), v(x_1), \ldots, v(x_N)\}$.*

Proof. Suppose $\alpha, \beta \in K^\times$ such that

$$v(\alpha) = \min\{v(x_0), v(x_1), \ldots, v(x_N)\} = v(\beta)$$

Then $v(\alpha) = v(\beta)$ and $\alpha\beta^{-1} \in R^\times$. So,

$$\begin{aligned}[\widetilde{\alpha^{-1}x_0}, \widetilde{\alpha^{-1}x_1}, \ldots, \widetilde{\alpha^{-1}x_N}] &= [\widetilde{\alpha\beta^{-1}\alpha^{-1}x_0}, \widetilde{\alpha\beta^{-1}\alpha^{-1}x_1}, \ldots, \widetilde{\alpha\beta^{-1}\alpha^{-1}x_N}] \\ &= [\widetilde{\beta^{-1}x_0}, \widetilde{\beta^{-1}x_1}, \ldots, \widetilde{\beta^{-1}x_N}].\end{aligned}$$

That is, the reduction of P modulo $\mathfrak{p}$ is well-defined. □

Example 3.4. Consider the point $P = \left[\frac{11}{30}, \frac{24}{49}, \frac{23}{135}\right] \in \mathbb{P}^2(\mathbb{Q})$. As examples, we will consider its reduction modulo 5, 7 and 11.

Before we can reduce P modulo 5, we must first multiply each coordinate by 5 to "clear the denominators", this gives us

$$P = \left[5 \cdot \frac{11}{30}, 5 \cdot \frac{24}{49}, 5 \cdot \frac{23}{135}\right] = \left[\frac{11}{6}, \frac{5 \cdot 24}{49}, \frac{23}{27}\right].$$

Now that P is in normalized coordinates, we find that $\widetilde{P} = [1, 0, 4] \pmod 5$.

If we want to reduce P modulo 7, this time, we must first multiply each coordinate by $7^2 = 49$ to "clear the denominators":

$$P = \left[49 \cdot \frac{11}{30}, 49 \cdot \frac{24}{49}, 49 \cdot \frac{23}{135}\right] = \left[\frac{11 \cdot 49}{30}, \frac{24}{1}, \frac{23 \cdot 49}{135}\right].$$

Then, reducing modulo 7, $\widetilde{P} = [0, 3, 0] \pmod 7$.

Lastly, we will reduce P modulo 11. Since each coordinate of P is a 11-adic integer and not all coordinates reduce to 0 modulo 11, P is already in normalized coordinates for this case. Thus, we can reduce immediately for $\widetilde{P} = [0, 7, 4] \pmod{11}$.

The proof of the following lemma relating reduction modulo $\mathfrak{p}$ to v-adic distance can be found in page 50 of [3].

Lemma 3.5. *Let points $P, Q \in \mathbb{P}^1(K)$. Then*

$$\widetilde{P} = \widetilde{Q} \iff \rho_v(P, Q) < 1.$$

We will use the above lemma to show that linear fractional transformations respect reduction modulo $\mathfrak{p}$.

Proposition 3.6. *Let $P, Q \in \mathbb{P}^1(K)$ and $f \in PGL_2(R)$. Then*

$$\widetilde{P} = \widetilde{Q} \iff \widetilde{f(P)} = \widetilde{f(Q)}.$$

Proof. The proof follows via the equivalences provided by Lemma 2.3 and Lemma 3.5:

$$\begin{aligned} \widetilde{P} = \widetilde{Q} &\iff \rho_v(P, Q) < 1 \\ &\iff \rho_v(f(P), f(Q)) < 1 \\ &\iff \widetilde{f(P)} = \widetilde{f(Q)} \end{aligned}$$

□

One may ask how necessary is it that f is in $PGL_2(R)$, in which case consider the following examples:

Examples 3.7. Take $f = \begin{pmatrix} 8 & 1 \\ 2 & 9 \end{pmatrix}$ so that $f \notin PGL_2(\mathbb{Z}_7)$. Let $P = [9, 5]$ and $Q = [4, 10]$ in $\mathbb{P}^1(\mathbb{Q}_7)$ so that $\widetilde{P} = [2, 5] = \widetilde{Q}$ in $\mathbb{P}^1(\mathbb{F}_7)$. But evaluating the reduction of f at each of P and Q gives

$$\begin{aligned} f(P) = [77, 63] = [11, 9] \equiv [2, 1] \pmod 7 \\ f(Q) = [42, 98] = [3, 7] \equiv [1, 0] \pmod 7. \end{aligned}$$

Thus $\widetilde{f(P)} \neq \widetilde{f(Q)}$.

As a second example, let $p > 2$ be a prime. Take $g = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. Again note that $g \notin PGL_2(\mathbb{Z}_p)$. Let $S = [1, p]$ and $T = [1, 0]$ in $\mathbb{P}^1(\mathbb{Q}_p)$ so that $\widetilde{S} = [1, 0] = \widetilde{T}$ in $\mathbb{P}^1(\mathbb{F}_p)$. Evaluating the reduction of f at each S and T gives us

$$\begin{aligned} f(S) = [p, p] = [1, 1] \\ f(T) = [p, 0] = [1, 0], \end{aligned}$$

and it is clear that $\widetilde{f(S)} \neq \widetilde{f(T)}$.

These two examples demonstrate the necessity of $f \in PGL_2(R)$ for Proposition 3.6.

The following proposition, compounded with Lemma 2.3, will allow us to change coordinates from points $P_1, P_2, P_3 \in \mathbb{P}^1(K)$ with distinct reductions to $0, 1, \infty$ without altering the underlying dynamics.

Proposition 3.8. *Let $P_1, P_2, P_3 \in \mathbb{P}^1(K)$ be points with distinct reductions $\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3}$. Then there exists a linear fractional transformation $f \in PGL_2(R)$ so that $P_1 \mapsto 0$, $P_2 \mapsto 1$, $P_3 \mapsto \infty$.*

Proof. Write each point $P_i = [X_i, Y_i]$ in normalized coordinates as per Definition 3.2. WLOG take $v(X_1) > v(Y_1)$, otherwise apply the map $\frac{Y}{X} \in PGL_2(R)$ to each P_i, reversing the coordinates. Since the coordinates for each point are normalized, it follows that $v(Y_1) = 0$, i.e. $Y_1 \in R^\times$. Then apply the map $\frac{Y_1X - X_1Y}{Y} \in PGL_2(R)$ to each P_i. Note that this map sets $P_1 = [0, 1]$.

By assumption, $\widetilde{P_3} \neq \widetilde{P_1} = [0, 1]$, so $v(X_3) = 0$. So, apply the map $\frac{X}{Y_3X - X_3Y} \in PGL_2(R)$ to each P_i. Note that this map leaves $P_1 = [0, 1]$ and sets $P_3 = [1, 0]$.

Lastly, since our assumption gives us that $\widetilde{P_2}$ has distinct reduction from $\widetilde{P_1} = [0, 1]$ and $\widetilde{P_3} = [1, 0]$, we must have $v(X_2) = v(Y_2) = 0$. Then apply the map $\frac{Y_2X}{X_2Y} \in PGL_2(R)$ to each P_i. Since this map fixes both P_1 and P_3 and sets $P_2 = [1, 1]$, the composition of the above maps gives the required map in $PGL_2(R)$. □

With the previous statements, we have established how to reduce points modulo $\mathfrak{p}$. We now ask how to reduce a rational map modulo $\mathfrak{p}$. To begin, let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map of degree d in the form

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

where $F(X, Y), G(X, Y) \in K[X, Y]$ are homogeneous polynomials of degree d.

Before we can define reduction of maps modulo $\mathfrak{p}$, we first define the normalization of a rational map.

Definition 3.9. Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map in the form $\phi(X, Y) = [F(X, Y), G(X, Y)]$, where $F, G \in K[X, Y]$ are homogeneous polynomials. Then we say the pair (F, G) is *normalized*, or ϕ is in *normalized form* if $F, G \in R[X, Y]$ and at least one coefficient of F or G belongs to $R^\times$ (recall notation from Definition 3.1). Equivalently (and analogously to point normalization), we say $\phi = [F, G]$ is *normalized* if the polynomials

$$\begin{aligned} F(X, Y) &= a_0X^d + a_1X^{d-1}Y + \cdots + a_{d-1}XY^{d-1} + a_dY^d \\ G(X, Y) &= b_0X^d + b_1X^{d-1}Y + \cdots + b_{d-1}XY^{d-1} + b_dY^d \end{aligned}$$

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

The rational map case is in fact completely analogous to the point case: By clearing the denominators of each a_i, b_j, we can find $c \in K^\times$ so that $[cF, cG]$ is normalized. Moreover, this value of c is unique up to multiplication by a unit.

Writing $\phi = [F, G]$ in normalized form, the reduction modulo $\mathfrak{p}$ is defined in the natural way.

Definition 3.10. Let $\phi = [F, G]$ be normalized with

$$\begin{aligned} F(X, Y) &= a_0X^d + a_1X^{d-1}Y + \cdots + a_{d-1}XY^{d-1} + a_dY^d \\ G(X, Y) &= b_0X^d + b_1X^{d-1}Y + \cdots + b_{d-1}XY^{d-1} + b_dY^d \end{aligned}$$

Then, the *reduction of ϕ modulo $\mathfrak{p}$* is

$$\begin{aligned} \widetilde{\phi}(X, Y) &= [\widetilde{F}(X, Y), \widetilde{G}(X, Y)] \\ &= [\widetilde{a_0}X^d + \cdots + \widetilde{a_d}Y^d, \widetilde{b_0}X^d + \cdots + \widetilde{b_d}Y^d]. \end{aligned}$$

That is, $\widetilde{\phi}$ is obtained by taking each coefficient a_i, b_j modulo $\mathfrak{p}$.

Since at least one of a_i, b_j is a unit (due to Definition 3.9), at least one of $\widetilde{F}$ or $\widetilde{G}$ is a non-zero homogeneous polynomial. So $\widetilde{\phi} : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ is well-defined. Moreover, analogously to Proposition 3.3, the reduction of a rational map is also independent of the choice of polynomials F and G.

However, as we will see, the existence of $\widetilde{\phi}$ need not imply that $\widetilde{\phi}$ is well-behaving.

Example 3.11. Consider the rational map

$$\psi(X, Y) = [pX^d, Y^d].$$

Note that $\deg(\psi) = d$, but its reduction modulo $\mathfrak{p}$ is $\widetilde{\psi} = [0, Y^d] = [0, 1]$. But $\widetilde{\psi} = [0, 1]$ is a constant map and does not provide us any information to lift back to study ψ.

4. Resultant

Although a rational map $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ is of form $\phi = [F(X, Y), G(X, Y)]$, where F and G share no common roots, upon reduction modulo $\mathfrak{p}$, they may acquire common roots in the residue field $R/\mathfrak{p}$. To understand this phenomenon, we look to develop a tool - called the resultant - that will help us determine the existence of common roots, given the coefficients of F and G.

As a stepping stone toward our main proposition regarding the resultant, we first prove the following equivalence.

Proposition 4.1. *Let K be a field and $A(X, Y)$ and $B(X, Y)$ be homogeneous polynomials of degrees n and m in $K[X, Y]$. Then the following statements are equivalent:*

- *(i) $A(X, Y)$ and $B(X, Y)$ have a common zero in $\mathbb{P}^1(\overline{K})$*
- *(ii) $A(X, Y)$ and $B(X, Y)$ have a common non-constant factor in the $K[X, Y]$*
- *(iii) There exists non-zero homogeneous polynomials $C, D \in K[X, Y]$ such that $A(X, Y) \cdot C(X, Y) = B(X, Y) \cdot D(X, Y)$ with $\deg(C) \leq m-1$ and $\deg(D) \leq n-1$.*

Note that here $\overline{K}$ denotes the algebraic closure of K.

Proof. Observe that $(i) \iff (ii)$ is immediate since the polynomial $\gcd(A, B) \in K[X, Y]$ vanishes at precisely the common zeroes between A and B in $\mathbb{P}^1(\overline{K})$.

It is also clear that $(ii) \implies (iii)$. If there exists some common factor G, e.g. $\gcd(A, B)$, such that G divides A and G divides B, then we can choose homogeneous polynomials C and D so that $A = G \cdot D$ and $B = G \cdot C$. Then $A \cdot C = B \cdot D$, that is (iii).

Lastly, it suffices to show that $(iii) \implies (i)$. Consider the equation $A(X, Y) \cdot C(X, Y) = B(X, Y) \cdot D(X, Y)$ with $\deg(C) \leq m - 1$ and $\deg(D) \leq n - 1$. Upon factoring both sides into linear factors in $\overline{K}[X, Y]$, we find that $A(X, Y)$ has n linear factors, while $D(X, Y)$ has at most $n - 1$ linear factors. By pigeonhole principle, $A(X, Y)$ must have at least one linear factor (in $\overline{K}(X, Y)$) in common with $B(X, Y)$. Thus they must also share a common zero in $\mathbb{P}^1(\overline{K})$. □

Now we introduce our main proposition on the resultant between two homogeneous polynomials, which extends the statements of Proposition 4.1.

Proposition 4.2. *Let K be a field and $A(X,Y)$ and $B(X,Y)$ be homogeneous polynomials over K of the form*

$$A(X,Y) = a_0X^n + a_1X^{n-1}Y + \cdots + a_nY^n$$
$$B(X,Y) = b_0X^m + b_1X^{m-1}Y + \cdots + b_mY^m$$

so that $\deg(A) = n$ *and* $\deg(B) = m$.

Then, there exists a polynomial, the resultant of A and B

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

in the coefficients of A and B with the following properties:

(a) $Res\,(A,B) = 0 \iff A, B$ *have common zero in* $\mathbb{P}^1(\overline{K})$

(b) If $a_0b_0 \neq 0$ *and A and B are factored as*

$$A(X,Y) = a_0\prod_{i=1}^{n}(X - \alpha_iY) \qquad B(X,Y) = b_0\prod_{j=1}^{m}(X - \beta_jY),$$

then $Res\,(A,B) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)$.

(c) There exists $F_X, G_X, F_Y, G_Y \in \mathbb{Z}[a_0, \ldots, a_n, b_0, \ldots, b_m][X,Y]$ *homogeneous polynomials in X and Y of degrees $m-1$ and $n-1$, respectively such that*

$$F_X(X,Y)\cdot A(X,Y) + G_X(X,Y)\cdot B(X,Y) = Res\,(A,B)\,X^{m+n-1}$$
$$F_Y(X,Y)\cdot A(X,Y) + G_Y(X,Y)\cdot B(X,Y) = Res\,(A,B)\,Y^{m+n-1}$$

Observe that Y does not appear in the first equation and X does not appear in the second equation.

(d) The resultant is equal to the $(m+n)\times(m+n)$ determinant

$$Res\,(A,B) = \det\begin{vmatrix} a_0 & a_1 & \cdots & a_n & 0 & \cdots & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_n & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \ddots & \ldots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ldots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & \cdots & b_m & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ldots & \ldots & \ddots & \ddots & \vdots \\ 0 & \cdots & b_0 & b_1 & \cdots & \cdots & b_m & 0 \\ 0 & \cdots & 0 & b_0 & b_1 & \cdots & \cdots & b_m \end{vmatrix}$$

Thus $Res\,(A,B)$ is homogeneous of degree m in variables $a_0, \ldots, a_n$ (coefficients of A) and homogeneous of degree n in variables $b_0, \ldots, b_m$ (coefficients of B).

The proof of Proposition 4.2 follows from Proposition 4.1 and can be found on pages 54-56 of [3].

Remark 4.3. We can see immediately that

$$\widetilde{\mathrm{Res}\,(F,G)} = \mathrm{Res}\left(\widetilde{F}, \widetilde{G}\right).$$

since the resultant $\operatorname{Res}(F,G)$ is a polynomial in the coefficients of F and G, which when reduced, is exactly $\operatorname{Res}\left(\widetilde{F},\widetilde{G}\right)$.

Now that we have established the resultant between two homogeneous polynomials, we define the resultant of a rational map in the obvious way.

Definition 4.4. Let K be a field with non-archimedean absolute value $|\cdot|_v$ and let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map. Writing $\phi = [F,G]$ with normalized homogeneous polynomials $F, G \in R[X,Y]$, the *resultant of* ϕ is $\operatorname{Res}(\phi) := \operatorname{Res}(F,G)$.

Remark 4.5. If $\deg(\phi) = d$, then $\operatorname{Res}(\phi)$ is well-defined up to multiplication by α^{2d}, for $\alpha \in R^\times$, since $[F,G] = [uF,uG]$ for $u \in R^\times$.

It turns out that the resultant of ϕ provides an upper bound for the expansion of ϕ with respect to ρ_v. In fact, a rational map is always Lipschitz with respect to ρ_v.

Theorem 4.6. *Let K be a field with non-archimedean absolute value $|\cdot|_v$ and $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map. Then,*

$$\rho_v(\phi(P),\phi(Q)) \leq \frac{1}{|Res\,(\phi)|_v^2} \cdot \rho_v(P,Q)$$

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

Proof. Let $\phi = [F(X,Y), G(X,Y)]$ be written in normalized form with $\deg(F) = \deg(G) = d$. Proposition 4.2(c) tells us that there exist homogeneous polynomials $F_X, G_X, F_Y, G_Y \in R[X,Y]$ such that

$$F_X(X,Y)\cdot A(X,Y) + G_X(X,Y)\cdot B(X,Y) = \operatorname{Res}(A,B)\,X^{2d-1} \tag{4.7}$$

$$F_Y(X,Y)\cdot A(X,Y) + G_Y(X,Y)\cdot B(X,Y) = \operatorname{Res}(A,B)\,Y^{2d-1} \tag{4.8}$$

Let $P = [x,y]$ be a point in $\mathbb{P}^1(K)$ in normalized form. Setting $[X,Y] = [x,y]$ and applying the ultrametric inequality to the equation 4.7:

$$\begin{aligned}\left|\operatorname{Res}(\phi)\,x^{2d-1}\right|_v &= |F_X(x,y)\cdot F(x,y) + G_X(x,y)\cdot G(x,y)|_v \\ &\leq \max\{|F_X(x,y)\cdot F(x,y)|_v, |G_X(x,y), G(x,y)|_v\} \\ &\leq \max\{|F_X(x,y)|_v, |G_X(x,y)|_v\}\cdot\max\{|F(x,y)|_v, |G(x,y)|_v\}\end{aligned}$$

Since F_X and G_X have integer coefficients and x and y also belong to R, it follows that $|F_X(x,y)|_v, |G_X(x,y)|_v \leq 1$ and thus

$$\left|\operatorname{Res}(\phi)\,x^{2d-1}\right|_v \leq \max\{|F(x,y)|_v, |G(x,y)|_v\}.$$

By applying the same steps to Equation 4.8, we find an analogous inequality for y

$$\left|\operatorname{Res}(\phi)\,y^{2d-1}\right|_v \leq \max\{|F(x,y)|_v, |G(x,y)|_v\}.$$

Since P is normalized (i.e. $\max\{|x|_v, |y|_v\} = 1$, we have

$$|\operatorname{Res}(\phi)|_v \leq \max\{|F(x,y)|_v, |G(x,y)|_v\}. \tag{4.9}$$

which gives us a bound on how divisible the pair F and G are by high powers of $\mathfrak{p}$.

Now let $P = [P_1, P_2]$ and $S = [S_1, S_2]$ be points of $\mathbb{P}^1(K)$ in normalized form, so $\rho_v(P, S) = |P_1S_2 - P_2S_1|_v$. Then,

$$\begin{aligned}\rho_v(\phi(P), \phi(S)) &= \frac{|F(P_1, P_2) \cdot G(S_1, S_2) - F(S_1, S_2) \cdot G(P_1, P_2)|_v}{\max\{|F(P_1, P_2)|_v, |G(P_1, P_2)|_v\} \cdot \max\{|F(S_1, S_2)|_v, |G(S_1, S_2)|_v\}} \\ &\leq \frac{|F(P_1, P_2) \cdot G(S_1, S_2) - F(S_1, S_2) \cdot G(P_1, P_2)|_v}{|\mathrm{Res}\,(\phi)|_v^2}\end{aligned}$$

by applying Equation 4.9.

Lastly, observe that, by induction, $F(P_1, P_2) \cdot G(S_1, S_2) - F(S_1, S_2) \cdot G(P_1, P_2)$ vanishes if $P_1S_2 = P_2S_1$. This implies that $P_1S_2 - P_2S_1$ divides the polynomial $F(P_1, P_2) \cdot G(S_1, S_2) - F(S_1, S_2) \cdot G(P_1, P_2)$ in $R[P_1, P_2, S_1, S_2]$, so

$$F(P_1, P_2) \cdot G(S_1, S_2) - F(S_1, S_2) \cdot G(P_1, P_2) = (P_1S_2 - P_2S_1) \cdot H(P_1, P_2, S_1, S_2)$$

for some polynomial $H(P_1, P_2, S_1, S_2) \in R[P_1, P_2, S_1, S_2]$. So,

$$\begin{aligned}\rho_v(\phi(P), \phi(S)) &\leq \frac{|(P_1S_2 - P_2S_1) \cdot H(P_1, P_2, S_1, S_2)|_v}{|\mathrm{Res}\,(\phi)|_v^2} \\ &\leq \frac{|P_1S_2 - P_2S_2|_v}{|\mathrm{Res}\,(\phi)|_v^2} \\ &= \frac{\rho_v(P, S)}{|\mathrm{Res}\,(\phi)|_v^2},\end{aligned}$$

that is, ϕ is Lipschitz with respect to the v-adic chordal metric. □

We also have the immediate corollary that a rational map ϕ is non-expanding if $\mathrm{Res}\,(\phi) \in R^\times$.

Corollary 4.10. *Let K be a field with non-archimedean absolute value $|\cdot|_v$ and $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map. If Res (ϕ) is a unit, then ϕ is non-expanding, i.e.*

$$\rho_v(\phi(P), \phi(Q)) \leq \rho_v(P, Q)$$

As we will see in the next section, the non-expandingness of a rational map ϕ is a characterizing property of well-behaving rational maps, that is, maps with "good reduction".

5. Good Reduction

Recall that in Example 3.11, we saw a poor-behaving rational map. In particular, we saw that $\deg(\psi) \neq \deg(\widetilde{\psi})$. In this section, we examine rational maps that maintain the same degree through reduction.

Theorem 5.1. *Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map in normalized form as $\phi = [F, G]$. Then the following are equivalent:*

(a) $\deg(\phi) = \deg(\widetilde{\phi})$
(b) $\widetilde{F}(X, Y) = 0 = \widetilde{G}(X, Y)$ *have no solutions* $[\alpha, \beta] \in \mathbb{P}^1(\overline{k})$ *(recall that* $k = R/\mathfrak{p}$ *and* $\overline{k}$ *is the algebraic closure of* k*)*
(c) $\mathrm{Res}\,(\phi) \in R^\times$
(d) $\mathrm{Res}\left(\widetilde{F}, \widetilde{G}\right) \neq 0$

A rational map ϕ satisfying these properties is said to have good reduction (modulo $\mathfrak{p}$).

Proof. Observe that $(b) \iff (c) \iff (d)$ follows immediately from Proposition 4.2 and Remark 4.3. To complete the proof, it suffices to show that $(a) \iff (b)$. Note that

$$\deg(\widetilde{\phi}) = \deg(\phi) - C$$

where C is the number of roots (counted according to multiplicity) that $\widetilde{F}$ and $\widetilde{G}$ have in common, which are erased by the reduction. In particular, $\deg(\phi) = \deg(\widetilde{\phi}) \iff \widetilde{F}, \widetilde{G}$ share no common roots. □

Recall that Corollary 4.10 required that $\mathrm{Res}\,(\phi) \in R^\times$. By Theorem 5.1, we now have the following (equivalent) formulation.

Corollary 5.2. *Let K be a field with non-archimedean absolute value $|\cdot|_v$ and $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map of good reduction. Then ϕ is non-expanding, i.e.*

$$\rho_v(\phi(P), \phi(Q)) \leq \rho_v(P, Q)$$

Next we consider some of the expected "good" properties of rational maps with good reduction.

Theorem 5.3. *Let K be a field and $\phi, \psi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be rational maps with good reduction. Then*

(a) $\widetilde{\phi(P)} = \widetilde{\phi}(\widetilde{P})$ for any point $P \in \mathbb{P}^1(K)$
(b) $\phi \circ \psi$ has good reduction and $\widetilde{\phi \circ \psi} = \widetilde{\phi} \circ \widetilde{\psi}$

The proof of this theorem can be found on page 59-60 of [3]. It is reasonable to ask whether if good reduction of a composition implies good reduction of the individual maps. However, this is not the case as we can find ϕ and ψ such that $\phi \circ \psi$ has good reduction but the maps alone have bad reduction, even after applying an element of $PGL_2(R)$.

As we wrap up our discussion of maps with good reduction themselves, we can begin our discussion of periodic points in maps of good reduction. To start off, we give the following fairly intuitive statement regarding where the reduction sends (pre-)periodic points.

Corollary 5.4. *Let K be a field and $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ a rational map with good reduction. Then*

$$Per(\phi) \to Per(\widetilde{\phi}) \qquad PrePer(\phi) \to PrePer(\widetilde{\phi}),$$

that is, $\widetilde{\cdot}$ sends periodic points in ϕ to periodic points in $\widetilde{\phi}$ and similarly for pre-periodic points.

Moreover, if $P \in Per(\phi)$ has period n and $\widetilde{P} \in Per(\widetilde{\phi})$ has period m, then m divides n.

Proof. Let P be periodic with period n, i.e. $P = \phi^n(P)$. Theorem 5.3 says that $\widetilde{P} = \widetilde{\phi^n(P)} = \widetilde{\phi}^n(\widetilde{P})$, that is $\widetilde{P}$ is periodic.

Now suppose $\widetilde{P}$ has period $m < n$, then $n = mk + r$, for some $0 \leq r < m$. Then

$$\widetilde{P} = \widetilde{\phi}^n(\widetilde{P}) = \widetilde{\phi}^r \circ \underbrace{\widetilde{\phi}^m \circ \widetilde{\phi}^m \circ \cdots \circ \widetilde{\phi}^m(\widetilde{P})}_{k \text{ times}} = \widetilde{\phi}^r(\widetilde{P})$$

Since $\widetilde{\phi}^r(\widetilde{P}) = \widetilde{P}$ and $r < m$, it follows that $r = 0$. Thus, m divides n and $\mathrm{Per}(\phi) \to \mathrm{Per}(\widetilde{\phi})$. The pre-periodic case follows via a similar argument. □

6. Periodic Points and Good Reduction

In preparation for this section and the next section, we will define some frequently used quantities.

Definition 6.1. For K a field with non-archimedean absolute value $|\cdot|_v$ and $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ a rational map, define the following quantities for $P \in \mathbb{P}^1(K)$ a periodic point:

$$\begin{aligned} n &= \text{period of } P \text{ for } \phi \\ m &= \text{period of } \widetilde{P} \text{ for } \widetilde{\phi} \\ r &= \text{order of } \lambda_{\widetilde{\phi}}(\widetilde{P}) = \left(\widetilde{\phi}\right)'(\widetilde{P}) \text{ in the multiplicative group } K^\times \\ &\qquad \text{As convention, take } r = \infty \text{ if } \lambda_{\widetilde{\phi}}(\widetilde{P})^n \neq 1 \text{ for all } n \\ p &= \text{char}(k), \text{ recall that } k = R/\mathfrak{p} \end{aligned}$$

In the previous section, Corollary 5.4 tells us that the period of a reduced periodic point for $\widetilde{\phi}$, m, divides the period of the periodic point for ϕ, n. But is there more we can say about the relationship between the two periods? The following theorem combines results of Li, Morton-Silverman, Narkiewicz, Pezda, and Zieve, to give us the possible forms $n = mk$ can take on.

Theorem 6.2. *Let K be a local field with non-archimedean absolute value $|\cdot|_v$. Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ a rational map with good reduction and $\deg(\phi) = d \geq 2$. Let $P \in \mathbb{P}^1(K)$ be a periodic point of ϕ with quantities defined in Definition 6.1. Then, n has one of the following forms*

$$n = \begin{cases} m \\ mr \\ mrp^e, \text{ for some } e \in \mathbb{Z}^+ \end{cases}$$

Proof. In this proof, we will be using the notation introduced in Definition 6.1

Recall from Theorem 5.3 that $\widetilde{\phi^i(Q)} = \widetilde{\phi}^i(\widetilde{Q})$ for all points $Q \in \mathbb{P}^1(K)$ and all $i \geq 0$. Also recall that Corollary 5.4 tells us that m divides n.

First we replace ϕ by ϕ^m and let $m = 1$, which reduces to the case where $\widetilde{P}$ is a fixed point of $\widetilde{\phi}$. Moreover, observe that $\lambda_{\widetilde{\phi}}(\widetilde{P}) = \widetilde{\phi}'(\widetilde{\phi}) = \widetilde{\phi'(P)}$. If P is a fixed point of ϕ, i.e. $\phi(P) = P$, then $n = m$ and we are done.

Now suppose that $\phi(P) \neq P$. Proposition 3.8 tells us that there exists $f \in PGL_2(R)$ such that $f([0,1]) = P$. WLOG we assume that $P = [0,1]$; otherwise, replace P by $f^{-1}(P) = [0,1]$ and ϕ by $\phi^f = f^{-1} \circ \phi \circ f$.

Dehomogenizing $z = \frac{X}{Y}$, we write

$$\phi(z) = \frac{a_d + a_{d-1}z + \cdots + a_1 d^{d-1} + a_0 z^d}{b_d + b_{d-1}z + \cdots + b_1 d^{d-1} + b_0 z^d}$$

where the coefficients $a_0, \ldots, a_d, b_0, \ldots, b_d \in R$ and at least one coefficient belongs to $R^\times$. Since our point $P = [0,1]$ is a fixed point of $\widetilde{\phi}$ and *phi* has good reduction, it follows that $\phi(0) = \frac{a_d}{b_d} \equiv 0 \pmod{\mathfrak{p}}$. Thus, $a_d \in \mathfrak{p}$ and $b_d \in R^\times$ and thus has an inverse. Multiplying the numerator and denominator by $b_d^{-1} \neq 0$, we can write ϕ

in the following form (Note that the coefficients may have changed)

$$\phi(z) = \frac{a_d + a_{d-1}z + \cdots + a_1 d^{d-1} + a_0 z^d}{1 + b_{d-1}z + \cdots + b_1 d^{d-1} + b_0 z^d}.$$

Consider the first few terms of the Taylor expansion of $\phi(z)$ around $z = 0$.

$$\phi(z) = \mu + \lambda z + \frac{A(z)}{1 + zB(z)} z^2$$

where $A(z), B(z) \in R[z]$, $\lambda = \phi'(0)$ and $\mu = a_d \in \mathfrak{p}$.

By induction, we see that

$$\phi^i(0) \equiv \mu(1 + \lambda + \lambda^2 + \cdots + \lambda^{i-1}) \pmod{\mu^2}$$

since the evaluation at 0 and taking the expression modulo μ^2 eliminates the cross-terms. In particular, since $\phi^n(0) = 0$ and $\mu = a_d \in \mathfrak{p}$, it follows that

$$1 + \lambda + \lambda^2 + \cdots + \lambda^{n-1} \equiv 0 \pmod{\mathfrak{p}}$$

Now we have two cases remaining. Recall that r is the order of $\lambda_{\widetilde{\phi}}(\widetilde{P})$ in $k^\times$ and observe that

$$\lambda_{\widetilde{\phi}}(\widetilde{P}) = 1 \iff r = 1.$$

First, we consider the case of $r \geq 2$, or equivalently, that $\lambda \not\equiv 1 \pmod{\mathfrak{p}}$. Then $\lambda^n \equiv 1 \pmod{\mathfrak{p}}$, which implies that r divides n. If $n = r$, we are done. Otherwise replace ϕ with ϕ^r and n with $\frac{n}{r}$. Then, again, we have ϕ in the form

$$\phi(z) = \mu + \lambda z + \frac{A(z)}{1 + zB(z)} z^2$$

possibly with different values of $\mu, \lambda, A(z)$ and $B(z)$.

This replacement of ϕ with ϕ^r and n with $\frac{n}{r}$ results in the second case, where $r = 1$, or equivalently $\lambda \equiv 1 \pmod{\mathfrak{p}}$. Recalling that

$$\begin{aligned} &\phi^n(0) = 0 \\ &\mu = \phi(0) = 0 \pmod{\mathfrak{p}} \\ &\lambda = \phi'(0) \equiv 1 \pmod{\mathfrak{p}} \end{aligned}$$

and assuming that $\phi(0) \neq 0$, it follows that

$$n \equiv 1 + \lambda + \lambda^2 + \cdots + \lambda^{d-1} \equiv 0 \pmod{\mathfrak{p}}$$

which implies that p divides n. Finally replace ϕ with ϕ^p and n with $\frac{n}{p}$. If we have achieved $\phi(0) = 0$ then we are done, otherwise, inductively repeat the replacing process until $n = 1$ and we can write $n = mrp^e$, for some $e \geq 1$. □

Recall that Corollary 4.10 tells us that maps with good reduction are non-expanding. This fact also allows us to conclude that all the periodic points of such well-behaving maps are also non-repelling.

Corollary 6.3. *Let K be a field and $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ a rational map with good reduction. Then every periodic point of ϕ is non-repelling.*

Proof. Since ϕ has good reduction, it follows from Theorem 5.3 that ϕ^n also has good reduction. Let P be a periodic point of period n. Proposition 3.8 allows us

to change coordinates so that $P = [0, 1]$. Then writing ϕ^n in normalized form, that is $F, G \in R[z]$

$$\phi^n(z) = \frac{F(z)}{G(z)} = \frac{a_1 z + a_2 z^2 + \cdots + a_d z^d}{b_0 + b_1 z + \cdots + b_d z^d}.$$

Since ϕ^n has good reduction, by Theorem 5.1, $z = 0$ cannot be a common root of $\widetilde{F}$ and $\widetilde{G}$, so b_0 must belong to $R^\times$. Then it follows that

$$\lambda_p(\phi) = (\phi^n)'(0) = \frac{a_1}{b_0} \in R$$

which implies that $|\lambda_p(\phi)|_v \leq 1$. So, P is a non-repelling periodic point. □

As we will see in greater detail in the next section, Theorem 6.2 is very powerful and will allow us to characterize the periods of periodic points depending on their leading coefficients in $\mathbb{P}^1(\mathbb{Q})$.

Next we look to find a bound on the set of periodic points of ϕ over K, $\mathrm{Per}(\phi, K)$.

Corollary 6.4. *Let K be a number field and $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ a rational map. Let $\mathfrak{p}$ and $\mathfrak{q}$ be primes of K that ϕ has good reduction on and $char(k_\mathfrak{p}) \neq char(k_\mathfrak{q})$, that is the characteristic of the residue fields are distinct. Then the period n of any periodic point of ϕ satisfies*

$$n \leq (N^2\mathfrak{p} - 1)(N^2\mathfrak{q} - 1)$$

where N denotes the norm.

Moreover, this tells us that the set $Per(\phi, K)$ of K-rational periodic points is finite.

We leave the details of the proof to be read on page 66 of [3].

Lastly we consider a theorem specific to $\mathbb{Q}_p$ and which provides insight on a specific case of Theorem 6.2.

Theorem 6.5. *Let $p \geq 5$ be a prime and let $K = \mathbb{Q}_p$. Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a rational map with good reduction and $P \in \mathbb{P}^1(K)$ be a periodic point such that $\widetilde{\phi}(\widetilde{P}) = \widetilde{P}$, that is $\widetilde{P}$ is a fixed point for $\widetilde{\phi}$, and $\widetilde{\phi}'(\widetilde{P}) = 1$.*

Then $\phi(P) = P$, that is P is also a fixed point for ϕ.

Observe that in the variables in 6.1, the above theorem states that is that $m = r = 1$ implies that $n = 1$ and $e = 0$. The proof of this theorem can be found on pages 67-69 of [3] and uses a similar argument to the proof of Theorem 6.2 via a Taylor expansion of ϕ.

7. Extended Example of $\phi(z) = [az^2 + bz + c, z^2]$

In this final section, we examine the rational map

$$\phi(z) = \frac{az^2 + bz + c}{z^2}$$

with $a, b, c \in \mathbb{Z}$. Suppose that $P \in \mathbb{P}^1(\mathbb{Q})$ is a periodic point of ϕ of period n. In particular, we want to determine the possible values n can take under various conditions. Note that we can also write ϕ in the form of a polynomial:

$$\phi\left(\frac{1}{z}\right) = cz^2 + bz + a$$

First we examine the case where $\gcd(c, 6)$, i.e. ϕ has good reduction for $\mathbb{Z}_2$ and $\mathbb{Z}_3$. Theorem 6.2 tells us that the period for ϕ has form $n = mrp^e$. We denote the period of $\widetilde{P}$ for $\widetilde{\phi}_2$ as m_2 and the order of $\lambda_{\widetilde{\phi}_2}(\widetilde{P})$ in $\mathbb{F}_2$ as r_2. We use similar notation for the $\mathbb{Z}_3$ case.

In the $\mathbb{Z}_2$ case we see that $\mathbb{P}^1(\mathbb{F}_2)$ has a total of 3 points, namely $[0,1], [1,1], \infty$ (we include ∞ since ϕ is a rational map). Thus $1 \leq m_2 \leq 3$. Moreover, since $k^\times = \mathbb{F}_2^\times$ has only one element, it follows that $r_2 = 1$ and $n = 3^s \cdot 2^{e_2}$, where $e_2 \geq 0$ and $s \leq 1$.

In the Z_3 case we perform a similar analysis: Since $\mathbb{P}^1(\mathbb{F}_3)$ has 4 points, namely $[0,1], [1,1], [2,1], \infty$, it follows that $1 \leq m_3 \leq 4$. Noting that $\mathbb{F}_3^\times$ has two elements, we find that $r_3 \leq 2$, so $n = 2^t \cdot 3^{e_3}$ for $t \leq 3$ and $e_3 \geq 0$.

Combining the results from the two cases, we conclude that $n = 2^t \cdot 3^s$, where $s \leq 1$ and $t \leq 3$, so $n \in \{1, 2, 3, 4, 6, 8, 12, 24\}$. But are all of these combinations actually possible?

It turns out that the only possible values of n are 1, 2, and 3. But why are the other options not feasible? Observe that if $n = 8$, we would require that $m_3 = 4$ and $r_3 = 2$. But suppose that $m_3 = 4$. Observe that in $\pmod 3$, we have the following mappings:

$$\begin{aligned}
\widetilde{\phi}_3(\infty) &= \widetilde{a} \\
\widetilde{\phi}_3(0) &= \infty \\
\widetilde{\phi}_3(1) &= \widetilde{a} + \widetilde{b} + \widetilde{c} \\
\widetilde{\phi}_3(2) &= \widetilde{a} - \widetilde{b} + \widetilde{c}
\end{aligned}$$

We determine the mappings $\widetilde{\phi}_3(1)$ and $\widetilde{\phi}_3(2)$ by noting that $z^2 \equiv 1 \pmod 3$ for $z = 1$ or 2 by Fermat's Little Theorem. In order of an $\widetilde{\phi}$ to achieve $m_3 = 4$, we must have that

$$0 \mapsto \infty \mapsto \widetilde{a} \mapsto \widetilde{\phi}(\widetilde{a}) \mapsto 0$$

This leaves $\widetilde{a}$ with two options: 1 or 2. If $\widetilde{a} = 1$, then we require that $\widetilde{\phi}(1) = 1 + \widetilde{b} + \widetilde{c} \equiv 2$ and $\widetilde{\phi}(2) = 0$. This gives us the pairs

$$(\widetilde{b}, \widetilde{c}) = \begin{cases} (0,1) & \text{but} \quad \widetilde{\phi}_3(2) = 1 - 0 + 1 = 2 \not\equiv 0 \\ (2,2) & \text{but} \quad \widetilde{\phi}_3(2) = 1 - 2 + 2 = 1 \not\equiv 0 \end{cases}$$

If instead, $\widetilde{a} = 2$, then we require that $\widetilde{\phi}(2) = 2 - \widetilde{b} + \widetilde{c} \equiv 1$ and $\widetilde{\phi}(1) = 0$. This gives us the pairs

$$(\widetilde{b}, \widetilde{c}) = \begin{cases} (0,2) & \text{but} \quad \widetilde{\phi}_3(1) = 2 + 0 + 2 = 1 \not\equiv 0 \\ (2,1) & \text{but} \quad \widetilde{\phi}_3(1) = 2 + 2 + 1 = 2 \not\equiv 0 \end{cases}$$

Thus $m_3 = 4$ does not occur.

In order to show that $n \neq 4, 6, 12, 24$, we note that all of these require $m_3 = 2$. With the assistance of some computer code, one can see that $m_3 = 2$ implies that $r = \infty$, or equivalently, $(\widetilde{\phi}_3^2)'(\widetilde{P}) = 0$.

Now, we will provide some examples of ϕ for the remaining viable values of $n = 1, 2, 3$. For $n = 1$, consider

$$\phi(z) = \frac{z^2 + z - 1}{z^2} \qquad z = 1$$

so that $\phi(1) = 1$. Next, for $n = 2$, observe that

$$\phi(z) = \frac{z^2 - z - 1}{z^2} \qquad z = 1$$

which maps 1 to -1 and back to 1. Lastly, for $n = 3$, take

$$\phi(z) = \frac{z^2 - 1}{z^2} \qquad z = 1$$

which produces the mapping $1 \mapsto 0 \mapsto \infty \mapsto 1$.

Acknowledgments

I would like to thank my mentor, Yulia Kotelnikova, for her assistance in the learning process and in particular, her patience in helping me understand the reading material in our weekly meetings. I am also very grateful for her advice on organizing and writing process. Next, I would like to thank Professor Hyde for providing me more intuition for understanding the p-adic numbers. Lastly, I would like to thank Professor May for again organizing the REU and its many talks as an opportunity to learn lots of interesting math.

References

[1] A. Mathew. The algebra and the arithmetic of quadratic forms. PCMI Undergraduate Summer School. July 15, 2021.
[2] T. Hyde. Office hour. July 19, 2021.
[3] J. H. Silverman. The Arithmetic of Dynamical Systems. Springer. 2007.