Arithmetic Dynamics

Joseph H. Silverman

Brown University

Workshop on p-adic Dynamics
Fields Institute, Toronto

Monday, October 27, 2008

What Is Dynamics?

A **(Discrete) Dynamical System** is simply a map

$$\boxed{\phi : S \longrightarrow S}$$

from a set to itself. Dynamics is the study of the behavior of the points in S under iteration of the map ϕ.

What Is Dynamics?

A **(Discrete) Dynamical System** is simply a map

$$\boxed{\phi : S \longrightarrow S}$$

from a set to itself. Dynamics is the study of the behavior of the points in S under iteration of the map ϕ.

We write

$$\phi^n = \underbrace{\phi \circ \phi \circ \phi \cdots \phi}_{n \text{ iterations}}$$

for the n^{th} iterate of ϕ and

$$\mathcal{O}_\phi(\alpha) = \{\alpha, \phi(\alpha), \phi^2(\alpha), \phi^3(\alpha), \ldots\}$$

for the **(forward) orbit of** $\alpha \in S$.

What Is Dynamics?

A **(Discrete) Dynamical System** is simply a map

$$\phi : S \longrightarrow S$$

from a set to itself. Dynamics is the study of the behavior of the points in S under iteration of the map ϕ.

We write

$$\phi^n = \underbrace{\phi \circ \phi \circ \phi \cdots \phi}_{n \text{ iterations}}$$

for the n^{th} iterate of ϕ and

$$\mathcal{O}_\phi(\alpha) = \{\alpha, \phi(\alpha), \phi^2(\alpha), \phi^3(\alpha), \ldots\}$$

for the **(forward) orbit of** $\alpha \in S$.

A primary goal in the study of dynamics is to classify the points of S according to the behavior of their orbits.

Polynomials and Rational Maps

The classical theory of dynamical systems studies how the iterates of polynomial and rational maps act on $\mathbb{R}$ or $\mathbb{C}$.

Polynomials and Rational Maps

The classical theory of dynamical systems studies how the iterates of polynomial and rational maps act on $\mathbb{R}$ or $\mathbb{C}$.

The *degree* of a *rational function*

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

is the larger of d and e.

Polynomials and Rational Maps

The classical theory of dynamical systems studies how the iterates of polynomial and rational maps act on $\mathbb{R}$ or $\mathbb{C}$.

The *degree* of a *rational function*

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

is the larger of d and e.

We will always assume that $\boxed{\deg(\phi) \geq 2}$.

Polynomials and Rational Maps

The classical theory of dynamical systems studies how the iterates of polynomial and rational maps act on $\mathbb{R}$ or $\mathbb{C}$.

The *degree* of a *rational function*

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

is the larger of d and e.

We will always assume that $\boxed{\deg(\phi) \geq 2}$.

A rational function is the same as a rational map (morphism)

$$\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$$

from the projective line to itself.

Some Dynamical Terminology

A point α is called **periodic** if

$$\phi^n(\alpha) = \alpha \quad \text{for some } n \geq 1.$$

The smallest such n is called the **period of** α.

Some Dynamical Terminology

A point α is called **periodic** if

$$\phi^n(\alpha) = \alpha \quad \text{for some } n \geq 1.$$

The smallest such n is called the **period of α**.

If $\phi(\alpha) = \alpha$, then α is a **fixed point**.

Some Dynamical Terminology

A point α is called **periodic** if

$$\phi^n(\alpha) = \alpha \quad \text{for some } n \geq 1.$$

The smallest such n is called the **period of α**.

If $\phi(\alpha) = \alpha$, then α is a **fixed point**.

A point α is **preperiodic** if some iterate $\phi^i(\alpha)$ is periodic, or equivalently, if its orbit $\mathcal{O}_\phi(\alpha)$ is finite.

Some Dynamical Terminology

A point α is called **periodic** if

$$\phi^n(\alpha) = \alpha \quad \text{for some } n \geq 1.$$

The smallest such n is called the **period of α**.

If $\phi(\alpha) = \alpha$, then α is a **fixed point**.

A point α is **preperiodic** if some iterate $\phi^i(\alpha)$ is periodic, or equivalently, if its orbit $\mathcal{O}_\phi(\alpha)$ is finite.

A **wandering point** is a point whose orbit is infinite.

Some Dynamical Terminology

A point α is called **periodic** if

$$\phi^n(\alpha) = \alpha \quad \text{for some } n \geq 1.$$

The smallest such n is called the **period of α**.

If $\phi(\alpha) = \alpha$, then α is a **fixed point**.

A point α is **preperiodic** if some iterate $\phi^i(\alpha)$ is periodic, or equivalently, if its orbit $\mathcal{O}_\phi(\alpha)$ is finite.

A **wandering point** is a point whose orbit is infinite.

An Example: The Map $\phi(z) = z^2$

- 2 and $\frac{1}{2}$ are *wandering points.*
- 0 and 1 are *fixed points.*
- -1 is a *preperiodic* point that is not periodic.
- $\frac{-1+\sqrt{-3}}{2}$ is a periodic point of period 2.

Arithmetic Dynamics

What is Arithmetic Dynamics?

Arithmetic Dynamics is a relatively new field in which classical problems in the theory of Diophantine equations and arithmetic geometry are transposed into the setting of dynamical systems.

What is Arithmetic Dynamics?

Arithmetic Dynamics is a relatively new field in which classical problems in the theory of Diophantine equations and arithmetic geometry are transposed into the setting of dynamical systems.

The following associations gives a flavor of the correspondence:

What is Arithmetic Dynamics?

Arithmetic Dynamics is a relatively new field in which classical problems in the theory of Diophantine equations and arithmetic geometry are transposed into the setting of dynamical systems.

The following associations gives a flavor of the correspondence:

Diophantine Equations		**Dynamical Systems**
rational and integral points on varieties	$\longleftrightarrow$	rational and integral points in orbits
torsion points on abelian varieties	$\longleftrightarrow$	periodic and preperiodic points of rational maps

What is Arithmetic Dynamics?

Arithmetic Dynamics is a relatively new field in which classical problems in the theory of Diophantine equations and arithmetic geometry are transposed into the setting of dynamical systems.

The following associations gives a flavor of the correspondence:

Diophantine Equations		**Dynamical Systems**
rational and integral points on varieties	$\longleftrightarrow$	rational and integral points in orbits
torsion points on abelian varieties	$\longleftrightarrow$	periodic and preperiodic points of rational maps

In the rest of this talk I'll survey some current areas of research in arithmetic dynamics.

Periodic Points from an Arithmetic Perspective

Periodic Points and Number Theory

For a dynamicist, the periodic points of ϕ are the real or complex numbers satisfying an equation

$$\phi^n(z) = z \quad \text{for some } n = 1, 2, 3, \ldots.$$

Periodic Points and Number Theory

For a dynamicist, the periodic points of ϕ are the real or complex numbers satisfying an equation

$$\phi^n(z) = z \quad \text{for some } n = 1, 2, 3, \ldots.$$

A number theorist asks:

What sorts of numbers may appear as periodic points?

Periodic Points and Number Theory

For a dynamicist, the periodic points of ϕ are the real or complex numbers satisfying an equation

$$\phi^n(z) = z \quad \text{for some } n = 1, 2, 3, \ldots.$$

A number theorist asks:

What sorts of numbers may appear as periodic points?

For example:

Question. Is it possible for a periodic point to be a rational number?

Periodic Points and Number Theory

For a dynamicist, the periodic points of ϕ are the real or complex numbers satisfying an equation

$$\phi^n(z) = z \quad \text{for some } n = 1, 2, 3, \ldots.$$

A number theorist asks:

What sorts of numbers may appear as periodic points?

For example:

Question. Is it possible for a periodic point to be a rational number?

The answer is obviously

Yes.

We've seen several examples. This leads to the. . .

Periodic Points and Number Theory

Query. How many periodic points may be rational?

Periodic Points and Number Theory

Query. How many periodic points may be rational?

This is a more interesting question. There are always infinitely many complex periodic points, and in many cases there are infinitely many real periodic points.

Among the infinitely many periodic points, how many may be rational numbers?

Periodic Points and Number Theory

Query. How many periodic points may be rational?

This is a more interesting question. There are always infinitely many complex periodic points, and in many cases there are infinitely many real periodic points.

Among the infinitely many periodic points, how many may be rational numbers?

The answer is given by a fundamental theorem:

Theorem. (Northcott 1949) A rational function $\phi(z) \in \mathbb{Q}(z)$ has only finitely many periodic points that are rational numbers. More generally, a morphism $\phi : \mathbb{P}^N \to \mathbb{P}^N$ defined over a number field K has only finitely many K-rational preperiodic points.

Proof (Sketch) of Northcott's Theorem

Proof. Every math talk should have one proof, so I'll sketch the (fairly elementary) proof of Northcott's result.

Proof (Sketch) of Northcott's Theorem

Proof. Every math talk should have one proof, so I'll sketch the (fairly elementary) proof of Northcott's result. An important tool in the proof is the **height** of a rational number p/q:

$$H\left(\frac{p}{q}\right) = \max\bigl\{|p|, |q|\bigr\}.$$

Notice that for any constant B, there are only finitely many rational numbers $\alpha \in \mathbb{Q}$ with height $H(\alpha) \leq B$.

Proof (Sketch) of Northcott's Theorem

Proof. Every math talk should have one proof, so I'll sketch the (fairly elementary) proof of Northcott's result. An important tool in the proof is the **height** of a rational number p/q:

$$H\left(\frac{p}{q}\right) = \max\bigl\{|p|, |q|\bigr\}.$$

Notice that for any constant B, there are only finitely many rational numbers $\alpha \in \mathbb{Q}$ with height $H(\alpha) \le B$.

Lemma. If $\phi(z)$ has degree d, then there is a constant $C = C_\phi > 0$ so that for all rational numbers $\beta \in \mathbb{Q}$,

$$H\bigl(\phi(\beta)\bigr) \ge C \cdot H(\beta)^d.$$

This is intuitively reasonable if you write out $\phi(z)$ as a ratio of polynomials. The tricky part is making sure there's not too much cancellation.

Proof (Sketch) of Northcott's Theorem

Suppose that α is periodic, say $\phi^n(\alpha) = \alpha$. We apply the lemma repeatedly:

$$\begin{aligned}
H\bigl(\phi(\alpha)\bigr) & & &\geq C \cdot H(\alpha)^d \\
H\bigl(\phi^2(\alpha)\bigr) &\geq C \cdot H\bigl(\phi(\alpha)\bigr)^d &&\geq C^{1+d} \cdot H(\alpha)^{d^2} \\
H\bigl(\phi^3(\alpha)\bigr) &\geq C \cdot H\bigl(\phi^2(\alpha)\bigr)^d &&\geq C^{1+d+d^2} \cdot H(\alpha)^{d^3} \\
&\vdots &&\vdots \\
H\bigl(\phi^n(\alpha)\bigr) &\geq C \cdot H\bigl(\phi^{n-1}(\alpha)\bigr)^d &&\geq C^{1+d+\cdots+d^{n-1}} \cdot H(\alpha)^{d^n}
\end{aligned}$$

Proof (Sketch) of Northcott's Theorem

Suppose that α is periodic, say $\phi^n(\alpha) = \alpha$. We apply the lemma repeatedly:

$$\begin{aligned}
H\bigl(\phi(\alpha)\bigr) & & &\ge C \cdot H(\alpha)^d \\
H\bigl(\phi^2(\alpha)\bigr) &\ge C \cdot H\bigl(\phi(\alpha)\bigr)^d & &\ge C^{1+d} \cdot H(\alpha)^{d^2} \\
H\bigl(\phi^3(\alpha)\bigr) &\ge C \cdot H\bigl(\phi^2(\alpha)\bigr)^d & &\ge C^{1+d+d^2} \cdot H(\alpha)^{d^3} \\
&\vdots & &\vdots \\
H\bigl(\phi^n(\alpha)\bigr) &\ge C \cdot H\bigl(\phi^{n-1}(\alpha)\bigr)^d & &\ge C^{1+d+\cdots+d^{n-1}} \cdot H(\alpha)^{d^n}
\end{aligned}$$

But $\phi^n(\alpha) = \alpha$, so we get

$$H(\alpha) = H\bigl(\phi^n(\alpha)\bigr) \ge C^{(d^n-1)/(d-1)} H(\alpha)^{d^n}.$$

Proof (Sketch) of Northcott's Theorem

Suppose that α is periodic, say $\phi^n(\alpha) = \alpha$. We apply the lemma repeatedly:

$$\begin{aligned}
H\bigl(\phi(\alpha)\bigr) & & &\geq C \cdot H(\alpha)^d \\
H\bigl(\phi^2(\alpha)\bigr) &\geq C \cdot H\bigl(\phi(\alpha)\bigr)^d & &\geq C^{1+d} \cdot H(\alpha)^{d^2} \\
H\bigl(\phi^3(\alpha)\bigr) &\geq C \cdot H\bigl(\phi^2(\alpha)\bigr)^d & &\geq C^{1+d+d^2} \cdot H(\alpha)^{d^3} \\
&\vdots & &\vdots \\
H\bigl(\phi^n(\alpha)\bigr) &\geq C \cdot H\bigl(\phi^{n-1}(\alpha)\bigr)^d & &\geq C^{1+d+\cdots+d^{n-1}} \cdot H(\alpha)^{d^n}
\end{aligned}$$

But $\phi^n(\alpha) = \alpha$, so we get

$$H(\alpha) = H\bigl(\phi^n(\alpha)\bigr) \geq C^{(d^n-1)/(d-1)} H(\alpha)^{d^n}.$$

Then a little bit of algebra yields

$$H(\alpha) \leq C^{-1/(d-1)}.$$

This proves that the rational periodic points have bounded height, hence there are only finitely many of them. QED

Rational Periodic Points

We now know that $\phi(z)$ has only finitely many rational periodic points. This raises the question:

$\boxed{\textbf{How many rational periodic points may } \phi(z) \textbf{ have?}}$

Rational Periodic Points

We now know that $\phi(z)$ has only finitely many rational periodic points. This raises the question:

How many rational periodic points may $\phi(z)$ have?

If we don't restrict the degree of ϕ, then we can get as many as we want. Simply take ϕ to have large degree and set

$$\phi(0)=1, \quad \phi(1)=2, \quad \phi(2)=3, \quad \dots, \quad \phi(n-1)=0.$$

This leads to a system of n linear equations for the coefficients of ϕ in the coefficients of ϕ, so if $\deg(\phi)>n$, we can solve for the coefficients of ϕ.

A Uniformity Conjecture

Hence in order to pose an interesting question, we should restrict attention to rational functions of a fixed degree.

A Uniformity Conjecture

Hence in order to pose an interesting question, we should restrict attention to rational functions of a fixed degree.

Uniform Boundedness Conjecture for Rational Periodic Points. (Morton–Silverman) Fix an integer $d \geq 2$. Then there is a constant $C(d)$ so that every rational function $\phi(z) \in \mathbb{Q}(z)$ of degree d has at most $C(d)$ rational periodic points.

A Uniformity Conjecture

Hence in order to pose an interesting question, we should restrict attention to rational functions of a fixed degree.

Uniform Boundedness Conjecture for Rational Periodic Points. (Morton–Silverman) Fix an integer $d \ge 2$. Then there is a constant $C(d)$ so that every rational function $\phi(z) \in \mathbb{Q}(z)$ of degree d has at most $C(d)$ rational periodic points.

More generally,

Uniform Boundedness Conjecture (D, N, d). There is a constant $C(D, N, d)$ so that for every number field $K/\mathbb{Q}$ of degree D and for every morphism $\phi : \mathbb{P}^N \to \mathbb{P}^N$ of degree d defined over K, we have

$$\#\bigl(\operatorname{PrePer}(\phi) \cap \mathbb{P}^N(K)\bigr) \le C(D, N, d).$$

Applications of the Uniformity Conjecture

- The special case $(D, N, d) = (1, 1, 4)$ implies uniform boundedness of torsion points on elliptic curves over $\mathbb{Q}$ (Mazur's theorem), and $(D, 1, 4)$ implies the same for number fields of degree D (Merel's theorem).

Applications of the Uniformity Conjecture

- The special case $(D, N, d) = (1, 1, 4)$ implies uniform boundedness of torsion points on elliptic curves over $\mathbb{Q}$ (Mazur's theorem), and $(D, 1, 4)$ implies the same for number fields of degree D (Merel's theorem).

- Fakhruddin has shown that the general conjecture implies uniform boundedness of torsion points on abelian varieties of dimension N.

Rational Periodic Points of $\phi_c(z) = z^2 + c$

Even for very simple families of polynomials such as

$$\phi_c(z) = z^2 + c,$$

very little is known about the possible periods of rational periodic points.

Rational Periodic Points of $\phi_c(z) = z^2 + c$

Even for very simple families of polynomials such as

$$\phi_c(z) = z^2 + c,$$

very little is known about the possible periods of rational periodic points.

We can write down some examples:

$\phi(z) = z^2$	has 1 as a point of period 1,
$\phi(z) = z^2 - 1$	has -1 as a point of period 2,
$\phi(z) = z^2 - \frac{29}{16}$	has $-\frac{1}{4}$ as a point of period 3,

Rational Periodic Points of $\phi_c(z) = z^2 + c$

Even for very simple families of polynomials such as

$$\phi_c(z) = z^2 + c,$$

very little is known about the possible periods of rational periodic points.

We can write down some examples:

$$\begin{array}{ll} \phi(z) = z^2 & \text{has } 1 \text{ as a point of period } 1, \\ \phi(z) = z^2 - 1 & \text{has } -1 \text{ as a point of period } 2, \\ \phi(z) = z^2 - \frac{29}{16} & \text{has } -\frac{1}{4} \text{ as a point of period } 3, \end{array}$$

Can $\phi(z) = z^2 + c$ have a rational point of period 4?

Rational Periodic Points of $\phi_c(z) = z^2 + c$

Theorem.
(a) There are many values of c such that $\phi_c(z)$ has a rational periodic point of period 1, 2, or 3.

(b) (Morton) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 4.

(c) (Flynn, Poonen, Schaefer) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 5.

(d) (Stoll) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 6 (conditional on the Birch–Swinnerton-Dyer conjecture).

Rational Periodic Points of $\phi_c(z) = z^2 + c$

Theorem.
(a) There are many values of c such that $\phi_c(z)$ has a rational periodic point of period 1, 2, or 3.

(b) (Morton) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 4.

(c) (Flynn, Poonen, Schaefer) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 5.

(d) (Stoll) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 6 (conditional on the Birch–Swinnerton-Dyer conjecture).

And that is the current state of our knowledge! No one knows if $\phi_c(z)$ can have rational periodic points of period 7 or greater. (Poonen has conjectured that it cannot.)

Integer Points in Orbits

Integers and Wandering Points

The orbit of a rational number α consists of rational numbers, so a natural number-theoretic question is to ask how often those rational numbers may be integers.

Question. Is it possible for an orbit $\mathcal{O}_\phi(\alpha)$ to contain infinitely many integers?

Integers and Wandering Points

The orbit of a rational number α consists of rational numbers, so a natural number-theoretic question is to ask how often those rational numbers may be integers.

> **Question.** Is it possible for an orbit $\mathcal{O}_\phi(\alpha)$ to contain infinitely many integers?

The obvious answer is **Yes**, of course it can. For example, take $\phi(z) = z^2 + 1$ and $\alpha = 1$.

Integers and Wandering Points

The orbit of a rational number α consists of rational numbers, so a natural number-theoretic question is to ask how often those rational numbers may be integers.

Question. Is it possible for an orbit $\mathcal{O}_\phi(\alpha)$ to contain infinitely many integers?

The obvious answer is **Yes**, of course it can. For example, take $\phi(z) = z^2 + 1$ and $\alpha = 1$.

More generally, if $\phi(z)$ is any polynomial with integer coefficients and if we start with an integer point, then the entire orbit consists of integers.

Are there any other possibilities?

Rational Functions with Polynomial Iterate

Here is an example of a nonpolynomial with an orbit containing infinitely many integer points. Let

$$\phi(z) = \frac{1}{z^d} \quad \text{and let} \quad \alpha \in \mathbb{Z}.$$

Then

$$\mathcal{O}_\phi(\alpha) = \left\{ \alpha, \frac{1}{\alpha^d}, \alpha^{d^2}, \frac{1}{\alpha^{d^3}}, \alpha^{d^4}, \frac{1}{\alpha^{d^5}}, \alpha^{d^6}, \ldots \right\}.$$

Thus half the points in the orbit are integers.

Rational Functions with Polynomial Iterate

Here is an example of a nonpolynomial with an orbit containing infinitely many integer points. Let

$$\phi(z) = \frac{1}{z^d} \quad \text{and let} \quad \alpha \in \mathbb{Z}.$$

Then

$$\mathcal{O}_\phi(\alpha) = \left\{ \alpha, \frac{1}{\alpha^d}, \alpha^{d^2}, \frac{1}{\alpha^{d^3}}, \alpha^{d^4}, \frac{1}{\alpha^{d^5}}, \alpha^{d^6}, \ldots \right\}.$$

Thus half the points in the orbit are integers.

This is not a surprising phenomenon, since $\phi^2(z) = z^{d^2}$ is a polynomial. And in principle, the same thing would happen if some higher iterate of ϕ were a polynomial. Somewhat surprisingly, this does not occur.

Rational Functions with Polynomial Iterate

Here is an example of a nonpolynomial with an orbit containing infinitely many integer points. Let

$$\phi(z) = \frac{1}{z^d} \quad \text{and let} \quad \alpha \in \mathbb{Z}.$$

Then

$$\mathcal{O}_\phi(\alpha) = \left\{ \alpha, \frac{1}{\alpha^d}, \alpha^{d^2}, \frac{1}{\alpha^{d^3}}, \alpha^{d^4}, \frac{1}{\alpha^{d^5}}, \alpha^{d^6}, \ldots \right\}.$$

Thus half the points in the orbit are integers.

This is not a surprising phenomenon, since $\phi^2(z) = z^{d^2}$ is a polynomial. And in principle, the same thing would happen if some higher iterate of ϕ were a polynomial. Somewhat surprisingly, this does not occur.

Theorem. If some iterate $\phi^n(z)$ is a polynomial, then already $\phi^2(z)$ is a polynomial.

Integer Points in Orbits

It turns out that the examples coming from polynomials are the only cases with orbits containing infinitely many integer points.

Integer Points in Orbits

It turns out that the examples coming from polynomials are the only cases with orbits containing infinitely many integer points.

Theorem. (Silverman) Let $\alpha \in \mathbb{Q}$ be a wandering point for ϕ, and assume that $\phi^2(z)$ is not a polynomial. Then the orbit $\mathcal{O}_\phi(\alpha)$ contain only finitely many integers.

Integer-Like Points in Wandering Orbits

There is a stronger, and more striking, description of the extent to which orbiting points fail to be integral.

Integer-Like Points in Wandering Orbits

There is a stronger, and more striking, description of the extent to which orbiting points fail to be integral. Start with some wandering $\alpha \in \mathbb{Q}$ and write the points in its orbit as fractions,

$$\phi^n(\alpha) = \frac{A_n}{B_n} \in \mathbb{Q} \qquad \text{for } n = 0, 1, 2, 3 \ldots.$$

Integer-Like Points in Wandering Orbits

There is a stronger, and more striking, description of the extent to which orbiting points fail to be integral. Start with some wandering $\alpha \in \mathbb{Q}$ and write the points in its orbit as fractions,

$$\phi^n(\alpha) = \frac{A_n}{B_n} \in \mathbb{Q} \qquad \text{for } n = 0, 1, 2, 3 \ldots.$$

Notice that $\phi^n(\alpha)$ is an integer if and only if $|B_n| = 1$. So the previous theorem says that $|B_n| \geq 2$ for $n > n_0$.

Integer-Like Points in Wandering Orbits

There is a stronger, and more striking, description of the extent to which orbiting points fail to be integral. Start with some wandering $\alpha \in \mathbb{Q}$ and write the points in its orbit as fractions,

$$\phi^n(\alpha) = \frac{A_n}{B_n} \in \mathbb{Q} \qquad \text{for } n = 0, 1, 2, 3 \ldots.$$

Notice that $\phi^n(\alpha)$ is an integer if and only if $|B_n| = 1$. So the previous theorem says that $|B_n| \geq 2$ for $n > n_0$.

Theorem. (Silverman) Assume that neither $\phi^2(z)$ nor $1/\phi^2(z^{-1})$ are polynomials and that $\alpha \in \mathbb{Q}$ has infinite orbit. Then

$$\lim_{n\to\infty} \frac{\log|A_n|}{\log|B_n|} = 1.$$

Integer-Like Points in Wandering Orbits

- This theorem is the dynanmical analogue of Siegel's theorem that curves of genus $g \geq 1$ have only finitely many integer points. The proof is an adaptation of Siegel's proof.

Integer-Like Points in Wandering Orbits

- This theorem is the dynanmical analogue of Siegel's theorem that curves of genus $g \geq 1$ have only finitely many integer points. The proof is an adaptation of Siegel's proof.
- However, the proof in the dynamical setting is more complicated because the map ϕ is always ramified, while Siegel was able to use unramified covering maps of curves.

Integer-Like Points in Wandering Orbits

- This theorem is the dynanmical analogue of Siegel's theorem that curves of genus $g \geq 1$ have only finitely many integer points. The proof is an adaptation of Siegel's proof.
- However, the proof in the dynamical setting is more complicated because the map ϕ is always ramified, while Siegel was able to use unramified covering maps of curves.
- Ultimately the proof reduces to a Diophantine approximation problem.

Integer-Like Points in Wandering Orbits

- This theorem is the dynanmical analogue of Siegel's theorem that curves of genus $g \geq 1$ have only finitely many integer points. The proof is an adaptation of Siegel's proof.
- However, the proof in the dynamical setting is more complicated because the map ϕ is always ramified, while Siegel was able to use unramified covering maps of curves.
- Ultimately the proof reduces to a Diophantine approximation problem.
- For particular functions and orbits it may be possible to give an elementary proof of finiteness, but I don't know a general proof that does not ultimately rely on Roth's theorem or one of its variants.

Additional Topics
in
Arithmetic Dynamics

Canonical Heights

Recall that a map ϕ of degree d more-or-less causes the height to be raised to the d^{th} power.

Canonical Heights

Recall that a map ϕ of degree d more-or-less causes the height to be raised to the d^{th} power.
For convenience, we introduce the **logarithmic height**

$$h\left(\frac{a}{b}\right) = \log H\left(\frac{a}{b}\right) = \log\max\bigl\{|a|,|b|\bigr\},$$

so

$$h\bigl(\phi(\alpha)\bigr) = dh(\alpha) + O(1).$$

Canonical Heights

Recall that a map ϕ of degree d more-or-less causes the height to be raised to the d^{th} power.
For convenience, we introduce the **logarithmic height**

$$h\left(\frac{a}{b}\right) = \log H\left(\frac{a}{b}\right) = \log\max\bigl\{|a|, |b|\bigr\},$$

so

$$h\bigl(\phi(\alpha)\bigr) = dh(\alpha) + O(1).$$

The **canonical height associated to ϕ** is

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

Canonical Heights

Recall that a map ϕ of degree d more-or-less causes the height to be raised to the d^{th} power.
For convenience, we introduce the **logarithmic height**

$$h\left(\frac{a}{b}\right) = \log H\left(\frac{a}{b}\right) = \log\max\bigl\{|a|,|b|\bigr\},$$

so

$$h\bigl(\phi(\alpha)\bigr) = dh(\alpha) + O(1).$$

The **canonical height associated to ϕ** is

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

One proves that the limit exists by using a telescoping sum argument to show that the sequence is Cauchy. (This idea is due to Tate.)

Properties of Canonical Heights

The canonical height has many nice properties:

Theorem.

(a) $\hat{h}_\phi(\alpha) = h(\alpha) + O(1)$.

(b) $\hat{h}_\phi\bigl(\phi(\alpha)\bigr) = d\hat{h}_\phi(\alpha)$.

(c) $\hat{h}_\phi(\alpha) \ge 0$.

(d) $\hat{h}_\phi(\alpha) = 0$ if and only if α is preperiodic.

Properties of Canonical Heights

The canonical height has many nice properties:

Theorem.
(a) $\hat{h}_\phi(\alpha) = h(\alpha) + O(1)$.
(b) $\hat{h}_\phi\bigl(\phi(\alpha)\bigr) = d\hat{h}_\phi(\alpha)$.
(c) $\hat{h}_\phi(\alpha) \ge 0$.
(d) $\hat{h}_\phi(\alpha) = 0$ if and only if α is preperiodic.

There are many conjectures about classical (canonical) heights that have analogs for dynamical heights, e.g.,

Dynamical Lehmer Conjecture. There is a constant $C = C(\phi) > 0$ so that for all algebraic numbers $\alpha \in \bar{\mathbb{Q}}$ that are not preperiodic for ϕ,

$$\hat{h}_\phi(\alpha) \ge \frac{C}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

A Dynamical Mordell Conjecture

Mordell's conjecture (Faltings' theorem) says that a curve of genus $g \geq 2$ has only finitely many rational points.

A Dynamical Mordell Conjecture

Mordell's conjecture (Faltings' theorem) says that a curve of genus $g \geq 2$ has only finitely many rational points.

A generalization (Bombieri-Lang Conjecture) says that the rational points on a variety of general type are sparse.

A Dynamical Mordell Conjecture

Mordell's conjecture (Faltings' theorem) says that a curve of genus $g \geq 2$ has only finitely many rational points.

A generalization (Bombieri-Lang Conjecture) says that the rational points on a variety of general type are sparse.

Using the analogy

$$\boxed{\text{Rational Points on Varieties}} \longleftrightarrow \boxed{\text{Points in Orbits}}$$

Dynamical Mordell Conjecture.
Let $\phi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism, let $\alpha \in \mathbb{P}^N$ be a wandering point for ϕ, and let $V \subset \mathbb{P}^N$ be a closed subvariety. Suppose

$$\mathcal{O}_\phi(\alpha) \cap V \text{ is infinite.}$$

Then there is a subvariety $W \subset V$ of dimension ≥ 1 that is preperiodic for ϕ, i.e, $\phi^{i+j}(W) \subset \phi^i(W)$.

A Dynamical Manin–Mumford Conjecture

The Manin–Mumford conjecture (Raynaud's theorem) says that if A is an abelian variety and if $V \subset A$ is a subvariety that contains infinitely many torsion points of A, then V contains a translate of an abelian subvariety of A.

A Dynamical Manin–Mumford Conjecture

The Manin–Mumford conjecture (Raynaud's theorem) says that if A is an abelian variety and if $V \subset A$ is a subvariety that contains infinitely many torsion points of A, then V contains a translate of an abelian subvariety of A.

Using the analogy

$$\boxed{\text{Torsion on Abelian Varieties}} \longleftrightarrow \boxed{\text{Preperiodic Points}}$$

Dynamical Manin–Mumford Conjecture.
Let $\phi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism and let $V \subset \mathbb{P}^N$ be a closed subvariety. Suppose

$$\operatorname{PrePer}(\phi) \cap V \text{ is infinite.}$$

Then there is a subvariety $W \subset V$ of dimension ≥ 1 that is preperiodic for ϕ.

Reduction Modulo p

A fundamental tool is *Reduction Modulo* p.

Reduction Modulo p

A fundamental tool is *Reduction Modulo p*.

Example. Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime for which E has *good reduction.* (This means that $\tilde{E}$ mod p is nonsingular.) Then

$$\bigl(\text{prime-to-}p\text{ torsion in } E(\mathbb{Q})\bigr) \hookrightarrow \tilde{E}(\mathbb{F}_p).$$

Reduction Modulo p

A fundamental tool is *Reduction Modulo p*.

Example. Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime for which E has *good reduction*. (This means that $\tilde{E}$ mod p is nonsingular.) Then

$$\big(\text{prime-to-}p \text{ torsion in } E(\mathbb{Q})\big) \hookrightarrow \tilde{E}(\mathbb{F}_p).$$

We want an analogous result in dynamics.

Reduction Modulo p

A fundamental tool is *Reduction Modulo p*.

Example. Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime for which E has *good reduction*. (This means that $\tilde{E}$ mod p is nonsingular.) Then

$$\bigl(\text{prime-to-}p \text{ torsion in } E(\mathbb{Q})\bigr) \hookrightarrow \tilde{E}(\mathbb{F}_p).$$

We want an analogous result in dynamics.

A map $\phi : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ of degree d has **good reduction** if the degree of the reduced map $\tilde{\phi} : \mathbb{P}^1_{\mathbb{F}_p} \to \mathbb{P}^1_{\mathbb{F}_p}$ is also d.

Reduction Modulo p

A fundamental tool is *Reduction Modulo p*.

Example. Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime for which E has *good reduction*. (This means that $\tilde{E} \bmod p$ is nonsingular.) Then

$$\bigl(\text{prime-to-}p\text{ torsion in } E(\mathbb{Q})\bigr) \hookrightarrow \tilde{E}(\mathbb{F}_p).$$

We want an analogous result in dynamics.

A map $\phi : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ of degree d has **good reduction** if the degree of the reduced map $\tilde{\phi} : \mathbb{P}^1_{\mathbb{F}_p} \to \mathbb{P}^1_{\mathbb{F}_p}$ is also d.

I.e., $\phi = F(z)/G(z)$ has good reduction if $\tilde{F}(z) \bmod p$ and $\tilde{G}(z) \bmod p$ have no common roots in $\bar{\mathbb{F}}_p$.

Reduction Modulo p

A fundamental tool is *Reduction Modulo p*.

Example. Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime for which E has *good reduction*. (This means that $\tilde{E}$ mod p is nonsingular.) Then

$$\bigl(\text{prime-to-}p\text{ torsion in }E(\mathbb{Q})\bigr) \hookrightarrow \tilde{E}(\mathbb{F}_p).$$

We want an analogous result in dynamics.

A map $\phi : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ of degree d has **good reduction** if the degree of the reduced map $\tilde{\phi} : \mathbb{P}^1_{\mathbb{F}_p} \to \mathbb{P}^1_{\mathbb{F}_p}$ is also d.

I.e., $\phi = F(z)/G(z)$ has good reduction if $\tilde{F}(z)$ mod p and $\tilde{G}(z)$ mod p have no common roots in $\bar{\mathbb{F}}_p$.

Equivalently, ϕ has good reduction if it extends to a scheme-theoretic morphism $\phi : \mathbb{P}^1_{\mathbb{Z}} \to \mathbb{P}^1_{\mathbb{Z}}$.

Reduction of Periodic Points Modulo p

Let $\phi : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be a rational map of degree d that has good reduction at p. Let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ be a periodic point of period n. The **multiplier of ϕ at α** is

$$\lambda_\alpha(\phi) = (\phi^n)'(\alpha).$$

Reduction of Periodic Points Modulo p

Let $\phi : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be a rational map of degree d that has good reduction at p. Let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ be a periodic point of period n. The **multiplier of ϕ at α** is

$$\lambda_\alpha(\phi) = (\phi^n)'(\alpha).$$

Theorem. Let

$$n = \text{period of } \alpha \text{ in } \mathbb{P}^1(\mathbb{Q}).$$
$$m = \text{period of } \tilde{\alpha} \bmod p \text{ in } \mathbb{P}^1(\mathbb{F}_p).$$
$$r = \text{order of } \lambda_\alpha(\tilde{\phi} \bmod p) \text{ in } \mathbb{F}_p^*.$$

Then

$$n = m \quad \text{or} \quad mr \quad \text{or} \quad mrp^e \quad \text{for some } e \geq 1.$$

Reduction of Periodic Points Modulo p

Let $\phi : \mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ be a rational map of degree d that has good reduction at p. Let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ be a periodic point of period n. The **multiplier of ϕ at α** is

$$\lambda_\alpha(\phi) = (\phi^n)'(\alpha).$$

Theorem. Let

$$n = \text{period of } \alpha \text{ in } \mathbb{P}^1(\mathbb{Q}).$$

$$m = \text{period of } \tilde{\alpha} \bmod p \text{ in } \mathbb{P}^1(\mathbb{F}_p).$$

$$r = \text{order of } \lambda_\alpha(\tilde{\phi} \bmod p) \text{ in } \mathbb{F}_p^*.$$

Then

$$n = m \quad \text{or} \quad mr \quad \text{or} \quad mrp^e \quad \text{for some } e \geq 1.$$

There is also a bound for e due to Zieve.

Application to Rational Periodic Points

Since

$$\#\mathbb{P}^1(\mathbb{F}_p) = p+1 \qquad \text{and} \qquad \#\mathbb{F}_p^* = p-1,$$

we clearly have

$$m \le p+1 \qquad \text{and} \qquad r \le p-1.$$

Hence

$$n = \text{period of } \alpha = Kp^e \quad \text{for some } K \le p^2 - 1.$$

Application to Rational Periodic Points

Since

$$\#\mathbb{P}^1(\mathbb{F}_p) = p + 1 \qquad \text{and} \qquad \#\mathbb{F}_p^* = p - 1,$$

we clearly have

$$m \le p + 1 \qquad \text{and} \qquad r \le p - 1.$$

Hence

$$n = \text{period of } \alpha = Kp^e \quad \text{for some } K \le p^2 - 1.$$

Corollary. Let p and q be the two smallest primes of good reduction for ϕ. Let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ be a periodic point. Then

$$(\text{period of } \alpha) \le (p^2 - 1)(q^2 - 1).$$

Application to Rational Periodic Points

Since

$$\#\mathbb{P}^1(\mathbb{F}_p) = p+1 \qquad \text{and} \qquad \#\mathbb{F}_p^* = p-1,$$

we clearly have

$$m \le p+1 \qquad \text{and} \qquad r \le p-1.$$

Hence

$$n = \text{period of } \alpha = Kp^e \quad \text{for some } K \le p^2 - 1.$$

Corollary. Let p and q be the two smallest primes of good reduction for ϕ. Let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ be a periodic point. Then

$$(\text{period of } \alpha) \le (p^2-1)(q^2-1).$$

With more work, one can significantly improve this estimate, but the bound will depend on ϕ.

Cyclotomic Fields

A **cyclotomic field** is a field extension of $\mathbb{Q}$ generated by roots of unity, i.e., by preperiodic points of the map $\phi(z) = z^2$.

Cyclotomic Fields

A **cyclotomic field** is a field extension of $\mathbb{Q}$ generated by roots of unity, i.e., by preperiodic points of the map $\phi(z) = z^2$.

Cyclotomic fields are important Galois extensions of $\mathbb{Q}$. Their Galios groups are abelian.

Cyclotomic Fields

A **cyclotomic field** is a field extension of $\mathbb{Q}$ generated by roots of unity, i.e., by preperiodic points of the map $\phi(z) = z^2$.

Cyclotomic fields are important Galois extensions of $\mathbb{Q}$. Their Galios groups are abelian.

Frobenius maps $z \longrightarrow z^p$ give reasonably good geometric control of the action of Galois.

Cyclotomic Fields

A **cyclotomic field** is a field extension of $\mathbb{Q}$ generated by roots of unity, i.e., by preperiodic points of the map $\phi(z) = z^2$.

Cyclotomic fields are important Galois extensions of $\mathbb{Q}$. Their Galios groups are abelian.

Frobenius maps $z \longrightarrow z^p$ give reasonably good geometric control of the action of Galois.

One can create **cyclotomic units** by taking expressions of the form

$$\frac{\zeta^i - \zeta^j}{\zeta^k - \zeta^\ell}.$$

The set of all cyclotomic units has finite index in the full unit group.

Dynamical "Cyclotomic" Fields

There is an analogous theory of **"dynatomic fields"** generated over $\mathbb{Q}$ by adjoining all of the points of period n.

Dynamical "Cyclotomic" Fields

There is an analogous theory of **"dynatomic fields"** generated over $\mathbb{Q}$ by adjoining all of the points of period n.

Dynatomic fields have Galois groups that are subgroups of wreath product groups.

Dynamical "Cyclotomic" Fields

There is an analogous theory of **"dynatomic fields"** generated over $\mathbb{Q}$ by adjoining all of the points of period n.

Dynatomic fields have Galois groups that are subgroups of wreath product groups.

There is some control of the action of Galois because ϕ acts as an element of Galois.

Dynamical "Cyclotomic" Fields

There is an analogous theory of **"dynatomic fields"** generated over $\mathbb{Q}$ by adjoining all of the points of period n.

Dynatomic fields have Galois groups that are subgroups of wreath product groups.

There is some control of the action of Galois because ϕ acts as an element of Galois.

One can create **dynatomic units** of the form

$$\boxed{\frac{\phi^i(\alpha) - \phi^j(\alpha)}{\phi^k(\alpha) - \phi^\ell(\alpha)}.}$$

Dynamical "Cyclotomic" Fields

There is an analogous theory of **"dynatomic fields"** generated over $\mathbb{Q}$ by adjoining all of the points of period n.

Dynatomic fields have Galois groups that are subgroups of wreath product groups.

There is some control of the action of Galois because ϕ acts as an element of Galois.

One can create **dynatomic units** of the form

$$\boxed{\frac{\phi^i(\alpha) - \phi^j(\alpha)}{\phi^k(\alpha) - \phi^\ell(\alpha)}}.$$

However, the dynatomic units generate only a portion of the full group of units.

Arithmetic Dynamics

Joseph H. Silverman

Brown University

Workshop on p-adic Dynamics
Fields Institute, Toronto

Monday, October 27, 2008

Moduli Spaces in Arithmetic Dynamics

Joseph H. Silverman

Brown University

Workshop on p-adic Dynamics
Fields Institute, Toronto

Tuesday, October 28, 2008

Parameter Spaces and Moduli Spaces

An enormously powerful tool throughout mathematics is the use of parameter spaces and moduli spaces.

Parameter Spaces and Moduli Spaces

An enormously powerful tool throughout mathematics is the use of parameter spaces and moduli spaces.
Let $\mathcal{C}$ be a collection of objects that we want to study and let $\sim$ be an equivalence relation on $\mathcal{C}$.

Parameter Spaces and Moduli Spaces

An enormously powerful tool throughout mathematics is the use of parameter spaces and moduli spaces.
Let $\mathcal{C}$ be a collection of objects that we want to study and let $\sim$ be an equivalence relation on $\mathcal{C}$.

Example: $\mathcal{C} = \{\text{elliptic curves over } \mathbb{C}\}$,
$\sim$ is isomorphism.

Parameter Spaces and Moduli Spaces

An enormously powerful tool throughout mathematics is the use of parameter spaces and moduli spaces.
Let $\mathcal{C}$ be a collection of objects that we want to study and let $\sim$ be an equivalence relation on $\mathcal{C}$.

Example: $\mathcal{C} = \{\text{elliptic curves over } \mathbb{C}\}$,
$\sim$ is isomorphism.

Very roughly speaking, a **parameter space** for $\mathcal{C}$ is a set with some additional structure whose points are in one-to-one correspondence with the points of $\mathcal{C}$.

Parameter Spaces and Moduli Spaces

An enormously powerful tool throughout mathematics is the use of parameter spaces and moduli spaces.
Let $\mathcal{C}$ be a collection of objects that we want to study and let $\sim$ be an equivalence relation on $\mathcal{C}$.

> Example: $\mathcal{C} = \{\text{elliptic curves over } \mathbb{C}\}$,
> $\sim$ is isomorphism.

Very roughly speaking, a **parameter space** for $\mathcal{C}$ is a set with some additional structure whose points are in one-to-one correspondence with the points of $\mathcal{C}$.

Similarly, a **moduli space** is a set with some additional structure whose points are in one-to-one correspondence with the set of equivalence classes $\mathcal{C}/\sim$.

Parameter Spaces and Moduli Spaces

An enormously powerful tool throughout mathematics is the use of parameter spaces and moduli spaces.

Let $\mathcal{C}$ be a collection of objects that we want to study and let $\sim$ be an equivalence relation on $\mathcal{C}$.

Example: $\mathcal{C} = \{\text{elliptic curves over } \mathbb{C}\}$,
$\sim$ is isomorphism.

Very roughly speaking, a **parameter space** for $\mathcal{C}$ is a set with some additional structure whose points are in one-to-one correspondence with the points of $\mathcal{C}$.

Similarly, a **moduli space** is a set with some additional structure whose points are in one-to-one correspondence with the set of equivalence classes $\mathcal{C}/\sim$.

The "additional structure" might be as a manifold or algebraic variety or scheme.

Moduli Spaces for Dynamical Systems

The Space of Rational Functions

The space of rational functions

$$\mathrm{Rat}_d = \{\text{rational maps } \mathbb{P}^1 \to \mathbb{P}^1 \text{ of degree } d\}$$

has a natural structure as an algebraic variety.

The Space of Rational Functions

The space of rational functions

$$\mathrm{Rat}_d = \{\text{rational maps } \mathbb{P}^1 \longrightarrow \mathbb{P}^1 \text{ of degree } d\}$$

has a natural structure as an algebraic variety.

To see this, we identify a rational map

$$\phi(z) = \frac{F_{\mathbf{a}}(z)}{F_{\mathbf{b}}(z)} = \frac{a_d z^d + \cdots + a_1 z + a_0}{b_d z^d + \cdots + b_1 z + b_0} \in \mathrm{Rat}_d$$

with a point in projective space,

$$[F_{\mathbf{a}}, F_{\mathbf{b}}] = [a_d, a_{d-1}, \ldots, a_0, b_d, b_{d-1}, \ldots, b_0] \in \mathbb{P}^{2d+1}.$$

The Space of Rational Functions

The space of rational functions

$$\mathrm{Rat}_d = \{\text{rational maps } \mathbb{P}^1 \to \mathbb{P}^1 \text{ of degree } d\}$$

has a natural structure as an algebraic variety.

To see this, we identify a rational map

$$\phi(z) = \frac{F_{\mathbf{a}}(z)}{F_{\mathbf{b}}(z)} = \frac{a_d z^d + \cdots + a_1 z + a_0}{b_d z^d + \cdots + b_1 z + b_0} \in \mathrm{Rat}_d$$

with a point in projective space,

$$[F_{\mathbf{a}}, F_{\mathbf{b}}] = [a_d, a_{d-1}, \ldots, a_0, b_d, b_{d-1}, \ldots, b_0] \in \mathbb{P}^{2d+1}.$$

The requirement that $\deg \phi = d$ is equivalent to

$$\mathrm{Resultant}(F_{\mathbf{a}}, F_{\mathbf{b}}) \neq 0,$$

so $\mathrm{Rat}_d \subset \mathbb{P}^{2d+1}$ is the complement of a hypersurface.

The Conjugation Action of $\mathrm{Aut}(\mathbb{P}^1)$

The dynamics of a rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ does not depend on a particular choice of coordinates. Let

$$f \in \mathrm{PGL}_2 = \mathrm{Aut}(\mathbb{P}^1)$$

be an automorphism of $\mathbb{P}^1$. The associated change of coordinates for ϕ is given by conjugation

$$\phi^f = f^{-1} \circ \phi \circ f.$$

The Conjugation Action of $\mathrm{Aut}(\mathbb{P}^1)$

The dynamics of a rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ does not depend on a particular choice of coordinates. Let

$$f \in \mathrm{PGL}_2 = \mathrm{Aut}(\mathbb{P}^1)$$

be an automorphism of $\mathbb{P}^1$. The associated change of coordinates for ϕ is given by conjugation

$$\phi^f = f^{-1} \circ \phi \circ f.$$

Thus we have a commutative diagram

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{\phi^f} & \mathbb{P}^1 \\ \Big\downarrow f & & \Big\downarrow f \\ \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^1 \end{array}$$

The Conjugation Action of $\mathrm{Aut}(\mathbb{P}^1)$

The dynamics of a rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ does not depend on a particular choice of coordinates. Let

$$f \in \mathrm{PGL}_2 = \mathrm{Aut}(\mathbb{P}^1)$$

be an automorphism of $\mathbb{P}^1$. The associated change of coordinates for ϕ is given by conjugation

$$\phi^f = f^{-1} \circ \phi \circ f.$$

Thus we have a commutative diagram

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{\phi^f} & \mathbb{P}^1 \\ \Big\downarrow f & & \Big\downarrow f \\ \mathbb{P}^1 & \xrightarrow{\phi} & \mathbb{P}^1 \end{array}$$

Notice that iteration of ϕ^f is given by

$$(\phi^f)^n = (f^{-1}\phi f)\cdots(f^{-1}\phi f) = f^{-1}\phi^n f = (\phi^n)^f.$$

Dynamical Moduli Spaces

Conjugation is the natural dynamical action of $\mathrm{PGL}_2 = \mathrm{Aut}(\mathbb{P}^1)$ on Rat_d, since the dynamical properties ϕ and ϕ^f are the same.

Dynamical Moduli Spaces

Conjugation is the natural dynamical action of $\mathrm{PGL}_2 = \mathrm{Aut}(\mathbb{P}^1)$ on Rat_d, since the dynamical properties ϕ and ϕ^f are the same.

Definition. The **moduli space** of dynamical systems of degree d is the quotient space

$$\mathcal{M}_d = \mathrm{Rat}_d \,/\, \mathrm{PGL}_2$$

of Rat_d by the conjugation action of PGL_2.

Dynamical Moduli Spaces

Conjugation is the natural dynamical action of $\mathrm{PGL}_2 = \mathrm{Aut}(\mathbb{P}^1)$ on Rat_d, since the dynamical properties ϕ and ϕ^f are the same.

Definition. The **moduli space** of dynamical systems of degree d is the quotient space

$$\mathcal{M}_d = \mathrm{Rat}_d \,/\, \mathrm{PGL}_2$$

of Rat_d by the conjugation action of PGL_2.

More generally, we can look at

$$\mathcal{M}_d^N = \mathrm{Rat}_d^N \,/\, \mathrm{PGL}_{N+1},$$

where

$$\mathrm{Rat}_d^N = \{\text{degree } d \text{ rational maps } \mathbb{P}^N \to \mathbb{P}^N\} \subset \mathbb{P}^L$$

and $\mathrm{PGL}_{N+1} = \mathrm{Aut}(\mathbb{P}^N)$ acts via conjugation.

Dynamical Moduli Spaces: Existence

It is not clear, *a priori*, that $\mathcal{M}_d$ exists as anything more than a set, but not surprisingly, we can endow $\mathcal{M}_d$ with a considerable amount of structure.

Dynamical Moduli Spaces: Existence

It is not clear, *a priori*, that $\mathcal{M}_d$ exists as anything more than a set, but not surprisingly, we can endow $\mathcal{M}_d$ with a considerable amount of structure.

Theorem. (a) (Milnor) *The quotient*

$$\mathcal{M}_d(\mathbb{C}) = \mathrm{Rat}_d(\mathbb{C}) / \mathrm{PGL}_2(\mathbb{C})$$

has a natural structure as a complex orbifold.

(b) (Silverman) *The quotient*

$$\mathcal{M}_d = \mathrm{Rat}_d / \mathrm{PSL}_2$$

has a natural structure as a scheme over $\mathbb{Z}$.

Dynamical Moduli Spaces: Existence

It is not clear, *a priori*, that $\mathcal{M}_d$ exists as anything more than a set, but not surprisingly, we can endow $\mathcal{M}_d$ with a considerable amount of structure.

Theorem. (a) (Milnor) *The quotient*

$$\mathcal{M}_d(\mathbb{C}) = \operatorname{Rat}_d(\mathbb{C}) / \operatorname{PGL}_2(\mathbb{C})$$

has a natural structure as a complex orbifold.

(b) (Silverman) *The quotient*

$$\mathcal{M}_d = \operatorname{Rat}_d / \operatorname{PSL}_2$$

has a natural structure as a scheme over $\mathbb{Z}$*.*

The construction of $\mathcal{M}_d$ as a variety, or as a scheme over $\mathbb{Z}$, uses Mumford's geometric invariant theory.

The Construction of the Moduli Space $\mathcal{M}_d$

Mumford's GIT provides larger sets of "stable" and "semistable" points and associated quotient spaces:

$$\mathrm{Rat}_d \subset \mathrm{Rat}_d^s \subset \mathrm{Rat}_d^{ss} \subset \mathbb{P}^{2d+1},$$
$$\mathcal{M}_d \subset \mathcal{M}_d^s \subset \mathcal{M}_d^{ss}.$$

The Construction of the Moduli Space $\mathcal{M}_d$

Mumford's GIT provides larger sets of "stable" and "semistable" points and associated quotient spaces:

$$\begin{aligned} &\mathrm{Rat}_d \subset \mathrm{Rat}_d^s \subset \mathrm{Rat}_d^{ss} \subset \mathbb{P}^{2d+1}, \\ &\mathcal{M}_d \subset \mathcal{M}_d^s \subset \mathcal{M}_d^{ss}. \end{aligned}$$

These quotients have various nice properties, such as:

$$\mathcal{M}_d^s(\mathbb{C}) = \frac{\mathrm{Rat}_d^s(\mathbb{C})}{\mathrm{PGL}_2(\mathbb{C})} \quad \text{and} \quad \mathcal{M}_d^{ss}(\mathbb{C}) \text{ is compact.}$$

The Construction of the Moduli Space $\mathcal{M}_d$

Mumford's GIT provides larger sets of "stable" and "semistable" points and associated quotient spaces:

$$\begin{aligned}&\mathrm{Rat}_d \subset \mathrm{Rat}_d^s \subset \mathrm{Rat}_d^{ss} \subset \mathbb{P}^{2d+1},\\ &\mathcal{M}_d \subset \mathcal{M}_d^s \subset \mathcal{M}_d^{ss}.\end{aligned}$$

These quotients have various nice properties, such as:

$$\mathcal{M}_d^s(\mathbb{C}) = \frac{\mathrm{Rat}_d^s(\mathbb{C})}{\mathrm{PGL}_2(\mathbb{C})} \quad \text{and} \quad \mathcal{M}_d^{ss}(\mathbb{C}) \text{ is compact.}$$

Proposition. *If d is even, then*

$$\mathcal{M}_d^s = \mathcal{M}_d^{ss},$$

so in this case there is a geometric quotient space that is a natural compactification $\mathcal{M}_d$.

For even d, we write $\overline{\mathcal{M}}_d$ for $\mathcal{M}_d^s = \mathcal{M}_d^{ss}$.

Dynamical Moduli Spaces: Properties

In general, little is known about the geometry of dynamical moduli spaces. Only for maps of degree two is there a complete description.

Dynamical Moduli Spaces: Properties

In general, little is known about the geometry of dynamical moduli spaces. Only for maps of degree two is there a complete description.

The complex orbifold structure of $\mathcal{M}_2$ turns out to be surprisingly simple.

Theorem. (Milnor)

$$\mathcal{M}_2(\mathbb{C}) \cong \mathbb{C}^2 \quad \text{and} \quad \overline{\mathcal{M}}_2(\mathbb{C}) \cong \mathbb{CP}^2.$$

Dynamical Moduli Spaces: Properties

In general, little is known about the geometry of dynamical moduli spaces. Only for maps of degree two is there a complete description.

The complex orbifold structure of $\mathcal{M}_2$ turns out to be surprisingly simple.

Theorem. (Milnor)

$$\mathcal{M}_2(\mathbb{C}) \cong \mathbb{C}^2 \quad \text{and} \quad \overline{\mathcal{M}}_2(\mathbb{C}) \cong \mathbb{CP}^2.$$

This structure carries over in the scheme-theoretic setting, even in characteristic 2.

Theorem. (Silverman)

$$\mathcal{M}_{2/\mathbb{Z}} \cong \mathbb{A}^2_{\mathbb{Z}} \quad \text{and} \quad \overline{\mathcal{M}}_{2/\mathbb{Z}} \cong \mathbb{P}^2_{\mathbb{Z}}.$$

An Explicit Isomorphism $\mathcal{M}_2 \cong \mathbb{A}^2$

The isomorphism

$$(\sigma_1, \sigma_2) : \mathcal{M}_2 \longrightarrow \mathbb{A}^2$$

may be given quite explicitly, although it is somewhat complicated. The image of a rational map

$$\phi = \frac{a_2 z^2 + a_1 z + a_0}{b_2 z^2 + b_1 z + b_0}$$

is given by the formulas

An Explicit Isomorphism $\mathcal{M}_2 \cong \mathbb{A}^2$

The isomorphism

$$(\sigma_1, \sigma_2) : \mathcal{M}_2 \longrightarrow \mathbb{A}^2$$

may be given quite explicitly, although it is somewhat complicated. The image of a rational map

$$\phi = \frac{a_2 z^2 + a_1 z + a_0}{b_2 z^2 + b_1 z + b_0}$$

is given by the formulas

$$\sigma_1 = \frac{\begin{array}{r} a_1^3 b_0 - 4a_0a_1a_2b_0 - 6a_2^2b_0^2 - a_0a_1^2b_1 + 4a_0^2a_2b_1 + 4a_1a_2b_0b_1 - 2a_0a_2b_1^2 \\ + a_2b_1^3 - 2a_1^2b_0b_2 + 4a_0a_2b_0b_2 - 4a_2b_0b_1b_2 - a_1b_1^2b_2 + 2a_0^2b_2^2 + 4a_1b_0b_2^2, \end{array}}{a_2^2b_0^2 - a_1a_2b_0b_1 + a_0a_2b_1^2 + a_1^2b_0b_2 - 2a_0a_2b_0b_2 - a_0a_1b_1b_2 + a_0^2b_2^2}$$

$$\sigma_2 = \frac{\begin{array}{r} -a_0^2a_1^2 + 4a_0^3a_2 - 2a_1^3b_0 + 10a_0a_1a_2b_0 + 12a_2^2b_0^2 - 4a_0^2a_2b_1 - 7a_1a_2b_0b_1 \\ - a_1^2b_1^2 + 5a_0a_2b_1^2 - 2a_2b_1^3 + 2a_0^2a_1b_2 + 5a_1^2b_0b_2 - 4a_0a_2b_0b_2 \\ - a_0a_1b_1b_2 + 10a_2b_0b_1b_2 - 4a_1b_0b_2^2 + 2a_0b_1b_2^2 - b_1^2b_2^2 + 4b_0b_2^3. \end{array}}{a_2^2b_0^2 - a_1a_2b_0b_1 + a_0a_2b_1^2 + a_1^2b_0b_2 - 2a_0a_2b_0b_2 - a_0a_1b_1b_2 + a_0^2b_2^2}$$

Multipliers of a Rational Map

A function on $\mathcal{M}_d$ is a function on Rat_d that is invariant under the action of PGL_2. We can construct such functions using multipliers.

Multipliers of a Rational Map

A function on $\mathcal{M}_d$ is a function on Rat_d that is invariant under the action of PGL_2. We can construct such functions using multipliers.

Let $\alpha \in \mathbb{P}^1$ be a periodic point of period n for ϕ. An easy chain rule calculation shows that the **multiplier**

$$\lambda_\phi(\alpha) = (\phi^n)'(\alpha)$$

is PGL_2-invariant, i.e.,

$$\lambda_f(\alpha) = \lambda_{\phi^f}(f^{-1}\alpha).$$

(If $\alpha = \infty$, the fomula for $\lambda_\phi(\alpha)$ is slightly different.)

Multipliers of a Rational Map

A function on $\mathcal{M}_d$ is a function on Rat_d that is invariant under the action of PGL_2. We can construct such functions using multipliers.

Let $\alpha \in \mathbb{P}^1$ be a periodic point of period n for ϕ. An easy chain rule calculation shows that the **multiplier**

$$\lambda_\phi(\alpha) = (\phi^n)'(\alpha)$$

is PGL_2-invariant, i.e.,

$$\lambda_f(\alpha) = \lambda_{\phi^f}(f^{-1}\alpha).$$

(If $\alpha = \infty$, the fomula for $\lambda_\phi(\alpha)$ is slightly different.)

We form combinations of $\lambda_\phi(\alpha)$ as α varies over the points of period n, a set we denote by

$$\mathrm{Per}_n(\phi) = \{\alpha \in \mathbb{P}^1 : \phi^n(\alpha) = \alpha\}.$$

Multiplier Systems

Let

$$\mathrm{Per}_n(\phi) = \{\alpha_1, \alpha_2, \ldots, \alpha_\rho\}, \qquad (\rho = d^n + 1),$$

where the α_i appear with multiplicities. We define

$$\sigma_n^{(i)} = \begin{pmatrix} i^{\text{th}} \text{ symmetric polynomial} \\ \text{in } \lambda_\phi(\alpha_1), \ldots, \lambda_\phi(\alpha_\rho) \end{pmatrix}.$$

Then each $\sigma_n^{(i)}(\phi)$ is a rational function in the coefficients $a_d, \ldots, a_0, b_d, \ldots, b_0$ of ϕ.

Multiplier Systems

Let
$$\mathrm{Per}_n(\phi) = \{\alpha_1, \alpha_2, \ldots, \alpha_\rho\}, \qquad (\rho = d^n + 1),$$
where the α_i appear with multiplicities. We define
$$\sigma_n^{(i)} = \begin{pmatrix} i^{\text{th}} \text{ symmetric polynomial} \\ \text{in } \lambda_\phi(\alpha_1), \ldots, \lambda_\phi(\alpha_\rho) \end{pmatrix}.$$

Then each $\sigma_n^{(i)}(\phi)$ is a rational function in the coefficients $a_d, \ldots, a_0, b_d, \ldots, b_0$ of ϕ.

Each $\sigma_n^{(i)}(\phi)$ is in the affine coordinate ring $\mathbb{Z}[\mathcal{M}_d]$, so they can be used to define a morphism
$$(\sigma_n^{(1)}, \sigma_n^{(2)}, \ldots, \sigma_n^{(\rho)}) : \mathcal{M}_d \longrightarrow \mathbb{A}^\rho.$$

Multiplier Systems

Let

$$\mathrm{Per}_n(\phi) = \{\alpha_1, \alpha_2, \ldots, \alpha_\rho\}, \qquad (\rho = d^n + 1),$$

where the α_i appear with multiplicities. We define

$$\sigma_n^{(i)} = \begin{pmatrix} i^{\text{th}} \text{ symmetric polynomial} \\ \text{in } \lambda_\phi(\alpha_1), \ldots, \lambda_\phi(\alpha_\rho) \end{pmatrix}.$$

Then each $\sigma_n^{(i)}(\phi)$ is a rational function in the coefficients $a_d, \ldots, a_0, b_d, \ldots, b_0$ of ϕ.

Each $\sigma_n^{(i)}(\phi)$ is in the affine coordinate ring $\mathbb{Z}[\mathcal{M}_d]$, so they can be used to define a morphism

$$(\sigma_n^{(1)}, \sigma_n^{(2)}, \ldots, \sigma_n^{(\rho)}) : \mathcal{M}_d \longrightarrow \mathbb{A}^\rho.$$

More generally, we can use periodic points of different periods to define a map

$$\boldsymbol{\sigma}_N = \left(\sigma_n^{(i)} : 1 \le n \le N,\ 1 \le i \le \rho_n\right) : \mathcal{M}_d \longrightarrow \mathbb{A}^L.$$

An Example: Rational Maps of Degree 2

The functions $\sigma_n^{(i)}$ are not independent. For example:

$$d = 2 \qquad \text{and} \qquad n = 1.$$

A rational map ϕ of degree two has three fixed points,

$$\operatorname{Per}_1(\phi) = \operatorname{FixedPoints}(\phi) = \{\alpha, \beta, \gamma\}.$$

An Example: Rational Maps of Degree 2

The functions $\sigma_n^{(i)}$ are not independent. For example:

$$d = 2 \qquad \text{and} \qquad n = 1.$$

A rational map ϕ of degree two has three fixed points,

$$\mathrm{Per}_1(\phi) = \mathrm{FixedPoints}(\phi) = \{\alpha, \beta, \gamma\}.$$

$$\begin{aligned}
\sigma_1^{(1)} &= \lambda(\alpha) + \lambda(\beta) + \lambda(\gamma), \\
\sigma_1^{(2)} &= \lambda(\alpha)\lambda(\beta) + \lambda(\alpha)\lambda(\gamma) + \lambda(\beta)\lambda(\gamma), \\
\sigma_1^{(3)} &= \lambda(\alpha)\lambda(\beta)\lambda(\gamma).
\end{aligned}$$

An elementary calculation shows that

$$\sigma_1^{(3)} = \sigma_1^{(1)} - 2,$$

and $\sigma_1^{(1)}, \sigma_1^{(2)}$ give the isomorphism described earlier:

$$(\sigma_1^{(1)}, \sigma_1^{(2)}) : \mathcal{M}_2 \xrightarrow{\ \sim\ } \mathbb{A}^2.$$

McMullen's Theorem

We might hope that sufficiently many of the $\sigma_n^{(i)}$ give an affine embedding of $\mathcal{M}_d$. This is not quite true.

McMullen's Theorem

We might hope that sufficiently many of the $\sigma_n^{(i)}$ give an affine embedding of $\mathcal{M}_d$. This is not quite true.

Theorem. (McMullen) If d is not a square, then for all sufficiently large N, the map

$$\boldsymbol{\sigma}_N : \mathcal{M}_d(\mathbb{C}) \longrightarrow \mathbb{C}^L$$

is finite-to-one.

If d is a square, the same is true except for a line that is mapped to a single point.

McMullen's Theorem

We might hope that sufficiently many of the $\sigma_n^{(i)}$ give an affine embedding of $\mathcal{M}_d$. This is not quite true.

Theorem. (McMullen) If d is not a square, then for all sufficiently large N, the map

$$\boldsymbol{\sigma}_N : \mathcal{M}_d(\mathbb{C}) \longrightarrow \mathbb{C}^L$$

is finite-to-one.

If d is a square, the same is true except for a line that is mapped to a single point.

As far as I know, this is still an open problem in characteristic p.

The Exceptional Set in McMullen's Theorem

The exceptional line in McMullen's Theorem is the set of Lattès maps. These are rational maps $\phi_{E,m}$ constructed from elliptic curves via diagrams

$$\begin{array}{ccc} E & \xrightarrow{[m]} & E \\ \big\downarrow x & & \big\downarrow x \\ \mathbb{P}^1 & \xrightarrow{\phi_{E,m}} & \mathbb{P}^1 \end{array}$$

For fixed m, the maps $\phi_{E,m}$ all have the same multipliers, but are not PGL_2-conjugate for non-isomorphic E.

The Exceptional Set in McMullen's Theorem

The exceptional line in McMullen's Theorem is the set of Lattès maps. These are rational maps $\phi_{E,m}$ constructed from elliptic curves via diagrams

$$\begin{array}{ccc} E & \xrightarrow{[m]} & E \\ \Big\downarrow x & & \Big\downarrow x \\ \mathbb{P}^1 & \xrightarrow{\phi_{E,m}} & \mathbb{P}^1 \end{array}$$

For fixed m, the maps $\phi_{E,m}$ all have the same multipliers, but are not PGL_2-conjugate for non-isomorphic E.

Using elliptic curves with complex mulitplication and the fact that class numbers of imaginary quadratic fields go to infinity, it is not hard to prove that the degree of

$$\boldsymbol{\sigma}_N : \mathcal{M}_d(\mathbb{C}) \longrightarrow \mathbb{C}^L$$

is unbounded as $d \to \infty$.

Questions Concerning the Geometry of $\mathcal{M}_d$

The space Rat_d is **rational**, which means that there is a generically 1-to-1 rational map

$$\mathbb{P}^{2d+1} \longrightarrow \mathrm{Rat}_d\,.$$

This is clear, since Rat_d is an open subset of $\mathbb{P}^{2d+1}$.

Questions Concerning the Geometry of $\mathcal{M}_d$

The space Rat_d is **rational**, which means that there is a generically 1-to-1 rational map

$$\mathbb{P}^{2d+1} \longrightarrow \mathrm{Rat}_d\,.$$

This is clear, since Rat_d is an open subset of $\mathbb{P}^{2d+1}$. It follows that $\mathcal{M}_d$ is **unirational**, i.e., there is a generically finite-to-1 rational map

$$\mathbb{P}^{2d-2} \longrightarrow \mathcal{M}_d.$$

Questions Concerning the Geometry of $\mathcal{M}_d$

The space Rat_d is **rational**, which means that there is a generically 1-to-1 rational map

$$\mathbb{P}^{2d+1} \longrightarrow \mathrm{Rat}_d\,.$$

This is clear, since Rat_d is an open subset of $\mathbb{P}^{2d+1}$.
It follows that $\mathcal{M}_d$ is **unirational**, i.e., there is a generically finite-to-1 rational map

$$\mathbb{P}^{2d-2} \longrightarrow \mathcal{M}_d.$$

Questions.
1. $\mathcal{M}_2 \cong \mathbb{A}_2$ is rational. Is $\mathcal{M}_3$ rational?
2. What do the singularities of $\mathcal{M}_d$ look like?
3. Let $\mathcal{M}_d(n)$ classify rational maps of degree d with a marked periodic point of period n. For fixed d, is $\mathcal{M}_d(n)$ of general type for sufficiently large n?
4. Same questions for the moduli spaces $\mathcal{M}_d^N$.

Lang's Height Conjecture

Conjecture. (Lang) Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})$ a nontorsion point. Then

$$\hat{h}(P) \ge c \log \bigl|\mathrm{Disc}(E/\mathbb{Q})\bigr|,$$

where $c > 0$ is an absolute constant.

Lang's Height Conjecture

Conjecture. (Lang) Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})$ a nontorsion point. Then

$$\hat{h}(P) \ge c \log \bigl| \operatorname{Disc}(E/\mathbb{Q}) \bigr|,$$

where $c > 0$ is an absolute constant.

Intuition: If E is arithmetically complicated, then its points are arithmetically complicated.

Lang's Height Conjecture

Conjecture. (Lang) Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})$ a nontorsion point. Then

$$\hat{h}(P) \ge c \log \bigl| \mathrm{Disc}(E/\mathbb{Q}) \bigr|,$$

where $c > 0$ is an absolute constant.

Intuition: If E is arithmetically complicated, then its points are arithmetically complicated.

Lang's conjecture has applications to the distribution of integer points on elliptic curves. Various weaker versions are known, and the conjecture has been proved conditional on the ABC-conjecture.

A Dynamical Analogue of Lang's Height Conjecture

We fix an embedding

$$\boxed{i_{\mathcal{M}} : \mathcal{M}_d \hookrightarrow \mathbb{P}^L}$$

and use it to define a height function

$$\boxed{h_{\mathcal{M}} : \mathcal{M}_d(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}, \qquad h_{\mathcal{M}}(\phi) = h\bigl(i_{\mathcal{M}}(\phi)\bigr).}$$

The height $h_{\mathcal{M}}(\phi)$ is a measure of the arithmetic complexity of the rational map ϕ.

A Dynamical Analogue of Lang's Height Conjecture

We fix an embedding

$$i_{\mathcal{M}} : \mathcal{M}_d \hookrightarrow \mathbb{P}^L$$

and use it to define a height function

$$h_{\mathcal{M}} : \mathcal{M}_d(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}, \qquad h_{\mathcal{M}}(\phi) = h\bigl(i_{\mathcal{M}}(\phi)\bigr).$$

The height $h_{\mathcal{M}}(\phi)$ is a measure of the arithmetic complexity of the rational map ϕ.

Conjecture. Fix a number field $K/\mathbb{Q}$. There is a constant $c > 0$, depending only on K and the embedding $\mathcal{M}_d \hookrightarrow \mathbb{P}^L$, such that for all maps $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree d and all wandering points $\alpha \in \mathbb{P}^1(K)$,

$$\hat{h}_\phi(\alpha) \geq c h_{\mathcal{M}}(\phi).$$

Dynamical Modular Curves

Dynatomic Polynomials

The $n^{\mathbf{th}}$ **cyclotomic polynomial**

$$\prod_{k|n}(z^k - 1)^{\mu(n/k)}$$

has as its roots the *primitive* n^{th}-roots of unity.

Dynatomic Polynomials

The $n^{\mathbf{th}}$ **cyclotomic polynomial**

$$\prod_{k|n}(z^k - 1)^{\mu(n/k)}$$

has as its roots the *primitive* n^{th}-roots of unity.

Similarly, the $n^{\mathbf{th}}$ **dynatomic polynomial** associated to a polynomial $\phi(z)$ is

$$\Phi_{\phi,n}(z) = \Phi_n(z) = \prod_{k|n}\bigl(\phi^n(z) - z\bigr)^{\mu(n/k)}.$$

Dynatomic Polynomials

The n^{th} **cyclotomic polynomial**

$$\prod_{k|n} (z^k - 1)^{\mu(n/k)}$$

has as its roots the *primitive* n^{th}-roots of unity.

Similarly, the n^{th} **dynatomic polynomial** associated to a polynomial $\phi(z)$ is

$$\Phi_{\phi,n}(z) = \Phi_n(z) = \prod_{k|n} \left(\phi^n(z) - z\right)^{\mu(n/k)}.$$

The roots α of $\Phi_\phi(z)$ are said to have **formal period n,** because although they satisfy

$$\phi^n(\alpha) = \alpha,$$

they occasionally have period strictly smaller than n. (This is different from the cyclotomic case.)

Dynatomic Polynomials (continued)

The polynomial $\phi^n(z) - z$ may have multiple roots. E.g.,

$$\phi(z) = z^2 - \frac{3}{4}, \quad \Phi_2 = \left(z + \frac{1}{2}\right)^2, \quad \phi\left(-\frac{1}{2}\right) = -\frac{1}{2}.$$

It is not clear that $\Phi_{\phi,n}(z)$ is a polynomial, but we have:

Dynatomic Polynomials (continued)

The polynomial $\phi^n(z)-z$ may have multiple roots. E.g.,

$$\phi(z) = z^2 - \frac{3}{4}, \quad \Phi_2 = \left(z + \frac{1}{2}\right)^2, \quad \phi\left(-\frac{1}{2}\right) = -\frac{1}{2}.$$

It is not clear that $\Phi_{\phi,n}(z)$ is a polynomial, but we have:

Theorem. The dynatomic "polynomial" is indeed a polynomial. Equivalently, for every point α,

$$\sum_{k|n} \mu(n/k) \operatorname{ord}_\alpha\bigl(\phi^n(z) - z\bigr) \geq 0.$$

Dynatomic Polynomials (continued)

The polynomial $\phi^n(z) - z$ may have multiple roots. E.g.,

$$\phi(z) = z^2 - \frac{3}{4}, \quad \Phi_2 = \left(z + \frac{1}{2}\right)^2, \quad \phi\left(-\frac{1}{2}\right) = -\frac{1}{2}.$$

It is not clear that $\Phi_{\phi,n}(z)$ is a polynomial, but we have:

Theorem. The dynatomic "polynomial" is indeed a polynomial. Equivalently, for every point α,

$$\sum_{k|n} \mu(n/k) \operatorname{ord}_\alpha\bigl(\phi^n(z) - z\bigr) \geq 0.$$

More generally, every rational map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ has an associated dynatomic polynomial $\Phi_{\phi,n}(X,Y)$. The roots of $\Phi_{\phi,n}$ define a **dynatomic divisor** in $\operatorname{Div}(\mathbb{P}^1)$, and the theorem says that this divisor is effective (positive).

The Dynatomic Polynomial of $z^2 + c$

We now restrict attention to the family of quadratic polynomials

$$\phi_c(z) = z^2 + c.$$

The Dynatomic Polynomial of $z^2 + c$

We now restrict attention to the family of quadratic polynomials

$$\phi_c(z) = z^2 + c.$$

Every quadratic polynomial can be put into this form via PGL_2-conjugation. The family $\{\phi_c\}$ has long been used as a testing ground for dynamical investigations.

The Dynatomic Polynomial of $z^2 + c$

We now restrict attention to the family of quadratic polynomials

$$\phi_c(z) = z^2 + c.$$

Every quadratic polynomial can be put into this form via PGL_2-conjugation. The family $\{\phi_c\}$ has long been used as a testing ground for dynamical investigations.

The n^{th}-dynatomic polynomial for ϕ_c is a polynomial in both z and c, so we will write it as

$$\Phi_n(c, z) \in \mathbb{Z}[z, c].$$

The Dynatomic Polynomial of $z^2 + c$

We now restrict attention to the family of quadratic polynomials

$$\phi_c(z) = z^2 + c.$$

Every quadratic polynomial can be put into this form via PGL_2-conjugation. The family $\{\phi_c\}$ has long been used as a testing ground for dynamical investigations.

The n^{th}-dynatomic polynomial for ϕ_c is a polynomial in both z and c, so we will write it as

$$\Phi_n(c, z) \in \mathbb{Z}[z, c].$$

$$\begin{aligned}
\Phi_1(c, z) &= z^2 - z + c \\
\Phi_2(c, z) &= z^2 + z + (c + 1) \\
\Phi_3(c, z) &= z^6 + z^5 + (3c + 1)z^4 + (2c + 1)z^3 + (3c^2 + 3c + 1)z^2 \\
&\quad + (c^2 + 2c + 1)z + (c^3 + 2c^2 + c + 1) \\
\Phi_6(c, z) &= z^{54} - z^{53} + 27cz^{52} + (-26c + 1)z^{51} + (351c^2 + 13c - 1)z^{50} + \cdots \\
&\quad + (c^{27} + 13c^{26} + 78c^{25} + 293c^{24} + 792c^{23} + \cdots + 3c^3 + c^2 - c + 1)
\end{aligned}$$

The Dynatomic Curve $Y_1^{\mathsf{dyn}}(n)$

The $n^{\mathbf{th}}$ **dynatomic curve** $Y_1^{\mathbf{dyn}}(n)$ is the affine curve defined by the equation

$$\Phi_n(y, z) = 0.$$

The Dynatomic Curve $Y_1^{\mathsf{dyn}}(n)$

The $n^{\mathbf{th}}$ **dynatomic curve** $Y_1^{\mathbf{dyn}}(n)$ is the affine curve defined by the equation

$$\boxed{\Phi_n(y,z) = 0.}$$

A point

$$\boxed{(c,\alpha) \in Y_1^{\mathrm{dyn}}(n)}$$

consists of a pair such that α is a periodic point of formal period n for the polynomial $\phi_c(z) = z^2 + c$.

The Dynatomic Curve $Y_1^{\mathsf{dyn}}(n)$

The $n^{\mathbf{th}}$ **dynatomic curve** $Y_1^{\mathbf{dyn}}(n)$ is the affine curve defined by the equation

$$\Phi_n(y, z) = 0.$$

A point

$$(c, \alpha) \in Y_1^{\mathrm{dyn}}(n)$$

consists of a pair such that α is a periodic point of formal period n for the polynomial $\phi_c(z) = z^2 + c$.

Notice the close analogy with the classical modular curve $Y_1(n)$ whose points classify pairs

$$(E, P)$$

consisting of an elliptic curve E and a point $P \in E$ of order n.

Rational Points on $Y_1^{\mathsf{dyn}}(n)$

A point $(c, \alpha) \in Y_1^{\text{dyn}}(n)$ classifies polynomials $z^2 + c$ with a point α of formal period n, and this classification respects the field of definition of the underlying object.

Rational Points on $Y_1^{\mathsf{dyn}}(n)$

A point $(c, \alpha) \in Y_1^{\text{dyn}}(n)$ classifies polynomials $z^2 + c$ with a point α of formal period n, and this classification respects the field of definition of the underlying object.

In particular, the set of rational points

$$\boxed{Y_1^{\text{dyn}}(n)(\mathbb{Q})}$$

classifies all quadratic polynomials with $\mathbb{Q}$-coefficients having a $\mathbb{Q}$-rational periodic point of (formal) period n.

Rational Points on $Y_1^{\mathsf{dyn}}(n)$

A point $(c, \alpha) \in Y_1^{\text{dyn}}(n)$ classifies polynomials $z^2 + c$ with a point α of formal period n, and this classification respects the field of definition of the underlying object.

In particular, the set of rational points

$$Y_1^{\text{dyn}}(n)(\mathbb{Q})$$

classifies all quadratic polynomials with $\mathbb{Q}$-coefficients having a $\mathbb{Q}$-rational periodic point of (formal) period n.

Thus the uniformity conjecture for quadratic polynomials is equivalent to the statement:

$$Y_1^{\text{dyn}}(n)(\mathbb{Q}) = \emptyset \quad \text{for sufficiently large } n,$$

and the strong uniformity conjecture asserts that

$$Y_1^{\text{dyn}}(n)(\mathbb{Q}) = \emptyset \qquad \text{for all } n \geq 4.$$

The Dynatomic Curve $X_1^{\mathsf{dyn}}(n)$

The curve $Y_1^{\mathrm{dyn}}(n)$ has a unique nonsingular completion, which we denote by $X_1^{\mathrm{dyn}}(n)$.

The Dynatomic Curve $X_1^{\mathsf{dyn}}(n)$

The curve $Y_1^{\mathrm{dyn}}(n)$ has a unique nonsingular completion, which we denote by $X_1^{\mathrm{dyn}}(n)$.

The finitely many points in the complement

$$X_1^{\mathrm{dyn}}(n) \smallsetminus Y_1^{\mathrm{dyn}}(n)$$

are called the **cusps** of $X_1^{\mathrm{dyn}}(n)$. They correspond to degenerations of the dynamical system $\phi_c(z) = z^2 + c$ and its marked point of formal period n.

The Dynatomic Curve $X_1^{\mathsf{dyn}}(n)$

The curve $Y_1^{\text{dyn}}(n)$ has a unique nonsingular completion, which we denote by $X_1^{\text{dyn}}(n)$.

The finitely many points in the complement

$$X_1^{\text{dyn}}(n) \setminus Y_1^{\text{dyn}}(n)$$

are called the **cusps** of $X_1^{\text{dyn}}(n)$. They correspond to degenerations of the dynamical system $\phi_c(z) = z^2 + c$ and its marked point of formal period n.

Theorem. (Bousch, Morton) The curve $X_1^{\text{dyn}}(n)$ is geometrically irreducible.

The Dynatomic Curve $X_1^{\mathsf{dyn}}(n)$

The curve $Y_1^{\mathrm{dyn}}(n)$ has a unique nonsingular completion, which we denote by $X_1^{\mathrm{dyn}}(n)$.

The finitely many points in the complement

$$X_1^{\mathrm{dyn}}(n) \setminus Y_1^{\mathrm{dyn}}(n)$$

are called the **cusps** of $X_1^{\mathrm{dyn}}(n)$. They correspond to degenerations of the dynamical system $\phi_c(z) = z^2 + c$ and its marked point of formal period n.

Theorem. (Bousch, Morton) The curve $X_1^{\mathrm{dyn}}(n)$ is geometrically irreducible.

The proofs are far from trivial and ultimately depend on dynamical arguments. (Remark: There are families for which the analogous dynatomic curves are reducible.)

The Dynatomic Curves $Y_0^{\mathsf{dyn}}(n)$ and $X_0^{\mathsf{dyn}}(n)$

There is a natural automorphism of $Y_1^{\mathrm{dyn}}(n)$ defined by

$$\begin{aligned} \hat{\phi} : Y_1^{\mathrm{dyn}}(n) &\longrightarrow & Y_1^{\mathrm{dyn}}(n), \\ (y,z) &\longmapsto & (y, z^2+y) = \bigl(y, \phi_y(z)\bigr). \end{aligned}$$

This automorphism extends to $X_1^{\mathrm{dyn}}(n)$.

The Dynatomic Curves $Y_0^{\mathsf{dyn}}(n)$ and $X_0^{\mathsf{dyn}}(n)$

There is a natural automorphism of $Y_1^{\mathrm{dyn}}(n)$ defined by

$$\begin{aligned} \hat{\phi} : Y_1^{\mathrm{dyn}}(n) &\longrightarrow \qquad\qquad Y_1^{\mathrm{dyn}}(n), \\ (y,z) &\longmapsto (y, z^2+y) = \bigl(y, \phi_y(z)\bigr). \end{aligned}$$

This automorphism extends to $X_1^{\mathrm{dyn}}(n)$.

Note that $\hat{\phi}^n = 1$. The quotients of $Y_1^{\mathrm{dyn}}(n)$ and $X_1^{\mathrm{dyn}}(n)$ by the action of $\hat{\phi}$ are denoted

$$\begin{aligned} Y_0^{\mathrm{dyn}}(n) &= Y_1^{\mathrm{dyn}}(n)/\hat{\phi}, \\ X_0^{\mathrm{dyn}}(n) &= X_1^{\mathrm{dyn}}(n)/\hat{\phi}. \end{aligned}$$

The Dynatomic Curves $Y_0^{\mathsf{dyn}}(n)$ and $X_0^{\mathsf{dyn}}(n)$

There is a natural automorphism of $Y_1^{\text{dyn}}(n)$ defined by

$$\begin{aligned} \hat{\phi} : Y_1^{\text{dyn}}(n) &\longrightarrow \qquad Y_1^{\text{dyn}}(n), \\ (y, z) &\longmapsto (y, z^2 + y) = \bigl(y, \phi_y(z)\bigr). \end{aligned}$$

This automorphism extends to $X_1^{\text{dyn}}(n)$.

Note that $\hat{\phi}^n = 1$. The quotients of $Y_1^{\text{dyn}}(n)$ and $X_1^{\text{dyn}}(n)$ by the action of $\hat{\phi}$ are denoted

$$\begin{aligned} Y_0^{\text{dyn}}(n) &= Y_1^{\text{dyn}}(n)/\hat{\phi}, \\ X_0^{\text{dyn}}(n) &= X_1^{\text{dyn}}(n)/\hat{\phi}. \end{aligned}$$

The points of $Y_0^{\text{dyn}}(n)$ classify pairs $(c, \mathcal{O})$, where $\mathcal{O}$ is the orbit of a point of formal period n for $\phi_c(z) = z^2 + c$.

The Genera of $X_1^{\mathsf{dyn}}(n)$ and $X_0^{\mathsf{dyn}}(n)$

Bousch and Morton found explicit, but rather messy, formulas for the genera of $X_1^{\mathrm{dyn}}(n)$ and $X_0^{\mathrm{dyn}}(n)$. The genera grow quite rapidly:

n	1	2	3	4	5	6	7	8	9	10
genus $X_1(n)$	0	0	0	2	14	34	124	285	745	1690
genus $X_0(n)$	0	0	0	0	2	4	16	32	79	162

The Genera of $X_1^{\mathsf{dyn}}(n)$ and $X_0^{\mathsf{dyn}}(n)$

Bousch and Morton found explicit, but rather messy, formulas for the genera of $X_1^{\mathrm{dyn}}(n)$ and $X_0^{\mathrm{dyn}}(n)$. The genera grow quite rapidly:

n	1	2	3	4	5	6	7	8	9	10
genus $X_1(n)$	0	0	0	2	14	34	124	285	745	1690
genus $X_0(n)$	0	0	0	0	2	4	16	32	79	162

Recall that Stoll proved (conditional on B–Sw-D):

Theorem. For $c \in \mathbb{Q}$, the polynomial $z^2 + c$ has no $\mathbb{Q}$-rational periodic point of exact period 6.

The Genera of $X_1^{\mathrm{dyn}}(n)$ and $X_0^{\mathrm{dyn}}(n)$

Bousch and Morton found explicit, but rather messy, formulas for the genera of $X_1^{\mathrm{dyn}}(n)$ and $X_0^{\mathrm{dyn}}(n)$. The genera grow quite rapidly:

n	1	2	3	4	5	6	7	8	9	10
genus $X_1(n)$	0	0	0	2	14	34	124	285	745	1690
genus $X_0(n)$	0	0	0	0	2	4	16	32	79	162

Recall that Stoll proved (conditional on B–Sw-D):

Theorem. For $c \in \mathbb{Q}$, the polynomial $z^2 + c$ has no $\mathbb{Q}$-rational periodic point of exact period 6.

The proof relies on the fact that the genus of $X_0^{\mathrm{dyn}}(6)$ is (barely) small enough to allow arithmetic computations.

Fields of Definition
and
Field of Moduli

The Map from Rat_d to $\mathcal{M}_d$

We let $\langle \quad \rangle$ denote the natural map

$$\langle \quad \rangle : \mathrm{Rat}_d \longrightarrow \mathcal{M}_d.$$

The Map from Rat_d to $\mathcal{M}_d$

We let $\langle\quad\rangle$ denote the natural map

$$\langle\quad\rangle : \mathrm{Rat}_d \longrightarrow \mathcal{M}_d.$$

Suppose that $\phi \in \mathrm{Rat}_d(\bar{\mathbb{Q}})$ satisfies

$$\langle\phi\rangle \in \mathcal{M}_d(\mathbb{Q}).$$

Note that this does not necessarily mean that ϕ itself is defined over $\mathbb{Q}$.

The Map from Rat_d to $\mathcal{M}_d$

We let $\langle\quad\rangle$ denote the natural map

$$\langle\quad\rangle : \mathrm{Rat}_d \longrightarrow \mathcal{M}_d.$$

Suppose that $\phi \in \mathrm{Rat}_d(\bar{\mathbb{Q}})$ satisfies

$$\langle\phi\rangle \in \mathcal{M}_d(\mathbb{Q}).$$

Note that this does not necessarily mean that ϕ itself is defined over $\mathbb{Q}$.

What it does mean is that for every $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, the map $\sigma(\phi)$ is $\mathrm{PGL}_2(\bar{\mathbb{Q}})$-conjugate to ϕ.

The Map from Rat_d to $\mathcal{M}_d$

We let $\langle\quad\rangle$ denote the natural map

$$\langle\quad\rangle : \mathrm{Rat}_d \longrightarrow \mathcal{M}_d.$$

Suppose that $\phi \in \mathrm{Rat}_d(\bar{\mathbb{Q}})$ satisfies

$$\langle\phi\rangle \in \mathcal{M}_d(\mathbb{Q}).$$

Note that this does not necessarily mean that ϕ itself is defined over $\mathbb{Q}$.

What it does mean is that for every $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, the map $\sigma(\phi)$ is $\mathrm{PGL}_2(\bar{\mathbb{Q}})$-conjugate to ϕ.

Question: Does this imply that there is some change of variables $f \in \mathrm{PGL}_2(\bar{\mathbb{Q}})$ such that

$$\phi^f \in \mathrm{Rat}_d(\mathbb{Q}).$$

Two Examples

Example 1. The polynomial

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

is not defined over $\mathbb{Q}$, but the change of variables

$$f(z) = z - \sqrt{2}$$

transforms it to

$$\phi^f(z) = f^{-1} \circ \phi \circ f(z) = \phi(z - \sqrt{2}) + \sqrt{2} = z^2 - 1.$$

Thus not only is

$$\langle \phi \rangle \in \mathcal{M}_2(\mathbb{Q}),$$

but we can find a change variables $f \in \mathrm{PGL}_2(\bar{\mathbb{Q}})$ such that

$$\phi^f \in \mathrm{Rat}_2(\mathbb{Q}).$$

Two Examples

Example 2. The rational map

$$\phi(z) = \sqrt{-1}\left(\frac{z-1}{z+1}\right)^3$$

has the property that

$$\overline{\phi}(z) = \phi^g(z) \qquad \text{with} \quad g(z) = -1/z,$$

where $\overline{}$ denotes complex conjugation.

Two Examples

Example 2. The rational map

$$\phi(z) = \sqrt{-1}\left(\frac{z-1}{z+1}\right)^3$$

has the property that

$$\overline{\phi}(z) = \phi^g(z) \qquad \text{with} \quad g(z) = -1/z,$$

where $\overline{}$ denotes complex conjugation.

On the other hand, it is not hard to prove that

$$\phi^f(z) \notin \mathrm{Rat}_d(\mathbb{Q}) \qquad \text{for all } f \in \mathrm{PGL}_2(\bar{\mathbb{Q}}).$$

Two Examples

Example 2. The rational map

$$\phi(z) = \sqrt{-1}\left(\frac{z-1}{z+1}\right)^3$$

has the property that

$$\overline{\phi}(z) = \phi^g(z) \qquad \text{with} \quad g(z) = -1/z,$$

where $\overline{}$ denotes complex conjugation.

On the other hand, it is not hard to prove that

$$\phi^f(z) \notin \mathrm{Rat}_d(\mathbb{Q}) \qquad \text{for all } f \in \mathrm{PGL}_2(\bar{\mathbb{Q}}).$$

Thus although ϕ seems as if it should be defined over $\mathbb{Q}$, it is not possible to change variables and make it actually defined over $\mathbb{Q}$.

Fields of Definition and Field of Moduli

Let $\phi \in \mathrm{Rat}_d(\bar{\mathbb{Q}})$.

Definition. A **Field of Definition** for ϕ is any field K for which there is an $f \in \mathrm{PGL}_2(\bar{\mathbb{Q}})$ such that

$$\phi^f \in \mathrm{Rat}_d(K).$$

Definition. The **Field of Moduli** of ϕ is the smallest field K such that

$$\langle\phi\rangle \in \mathcal{M}_d(K).$$

Fields of Definition and Field of Moduli

Let $\phi \in \mathrm{Rat}_d(\bar{\mathbb{Q}})$.

Definition. A **Field of Definition** for ϕ is any field K for which there is an $f \in \mathrm{PGL}_2(\bar{\mathbb{Q}})$ such that

$$\phi^f \in \mathrm{Rat}_d(K).$$

Definition. The **Field of Moduli** of ϕ is the smallest field K such that

$$\langle\phi\rangle \in \mathcal{M}_d(K).$$

Equivalently, let

$$G_\phi = \left\{\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) : \exists g \in \mathrm{PGL}_2(\bar{\mathbb{Q}}) \text{ with } \sigma(\phi) = \phi^g\right\}.$$

Then

$$K_\phi = \text{Field of Moduli of } \phi = \text{Fixed field of } G_\phi.$$

The Automorphism Group of a Rational Map

We are going to give a cohomological formulation for the question of whether the field of moduli is a field of definition:

$$\mathrm{FOM} = \mathrm{FOD}?$$

The Automorphism Group of a Rational Map

We are going to give a cohomological formulation for the question of whether the field of moduli is a field of definition:

$$\boxed{\mathrm{FOM} = \mathrm{FOD}?}$$

Definition. Let $\phi \in \mathrm{Rat}_d$. The **automorphism group of ϕ** (group of self-similarities) is

$$\boxed{\mathrm{Aut}(\phi) = \{f \in \mathrm{PGL}_2 : \phi^f = \phi\}.}$$

The Automorphism Group of a Rational Map

We are going to give a cohomological formulation for the question of whether the field of moduli is a field of definition:

$$\text{FOM} = \text{FOD?}$$

Definition. Let $\phi \in \mathrm{Rat}_d$. The **automorphism group of ϕ** (group of self-similarities) is

$$\mathrm{Aut}(\phi) = \{f \in \mathrm{PGL}_2 : \phi^f = \phi\}.$$

Example.

$$\phi = \frac{az}{bz^2 + c}, \qquad \mathrm{Aut}(\phi) = \{z, -z\}.$$

A Cohomological Criterion

We make the simplifying assumption that

$$\mathrm{Aut}(\phi) = 1.$$

Then for every $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K_\phi)$ there is a *unique* element $g_\sigma \in \mathrm{PGL}_2(\bar{\mathbb{Q}})$ satisfying

$$\sigma(\phi) = \phi^{g_\sigma}.$$

A Cohomological Criterion

We make the simplifying assumption that

$$\mathrm{Aut}(\phi) = 1.$$

Then for every $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K_\phi)$ there is a *unique* element $g_\sigma \in \mathrm{PGL}_2(\bar{\mathbb{Q}})$ satisfying

$$\sigma(\phi) = \phi^{g_\sigma}.$$

Proposition. (a) The map

$$\mathrm{Gal}(\bar{\mathbb{Q}}/K_\phi) \longrightarrow \mathrm{PGL}_2(\bar{\mathbb{Q}}), \qquad \sigma \longrightarrow g_\sigma,$$

is a 1-cocycle.

(b) The field of moduli K_ϕ is a field of definition for ϕ if and only if $\sigma \to g_\sigma$ is a coboundary, i.e.,

$$\mathrm{FOM} = \mathrm{FOD} \quad \Longleftrightarrow \quad [g_\sigma] = 0 \text{ in } H^1\bigl(\mathrm{Gal}, \mathrm{PGL}_2\bigr).$$

Some Cases of $\mathrm{FOM} = \mathrm{FOD}$

Using the cohomological criterion, one can prove the following.

Theorem. Let $\phi \in \mathrm{Rat}_d(\bar{\mathbb{Q}})$. Then

$$\boxed{\mathrm{FOM} = \mathrm{FOD} \;\text{ for } \phi}$$

in the following two situations:

(a) $\phi(z)$ has even degree.

(b) $\phi(z)$ is a polynomial.

Some Cases of $\mathrm{FOM} = \mathrm{FOD}$

Using the cohomological criterion, one can prove the following.

Theorem. Let $\phi \in \mathrm{Rat}_d(\bar{\mathbb{Q}})$. Then

$$\boxed{\mathrm{FOM} = \mathrm{FOD} \ \text{ for } \phi}$$

in the following two situations:

(a) $\phi(z)$ has even degree.

(b) $\phi(z)$ is a polynomial.

The theorem is true even in the case that $\mathrm{Aut}(\phi) \neq 1$, although the proof is more complicated.

Some Cases of $\mathrm{FOM} = \mathrm{FOD}$

Using the cohomological criterion, one can prove the following.

Theorem. Let $\phi \in \mathrm{Rat}_d(\bar{\mathbb{Q}})$. Then

$$\boxed{\mathrm{FOM} = \mathrm{FOD} \ \text{ for } \phi}$$

in the following two situations:

(a) $\phi(z)$ has even degree.

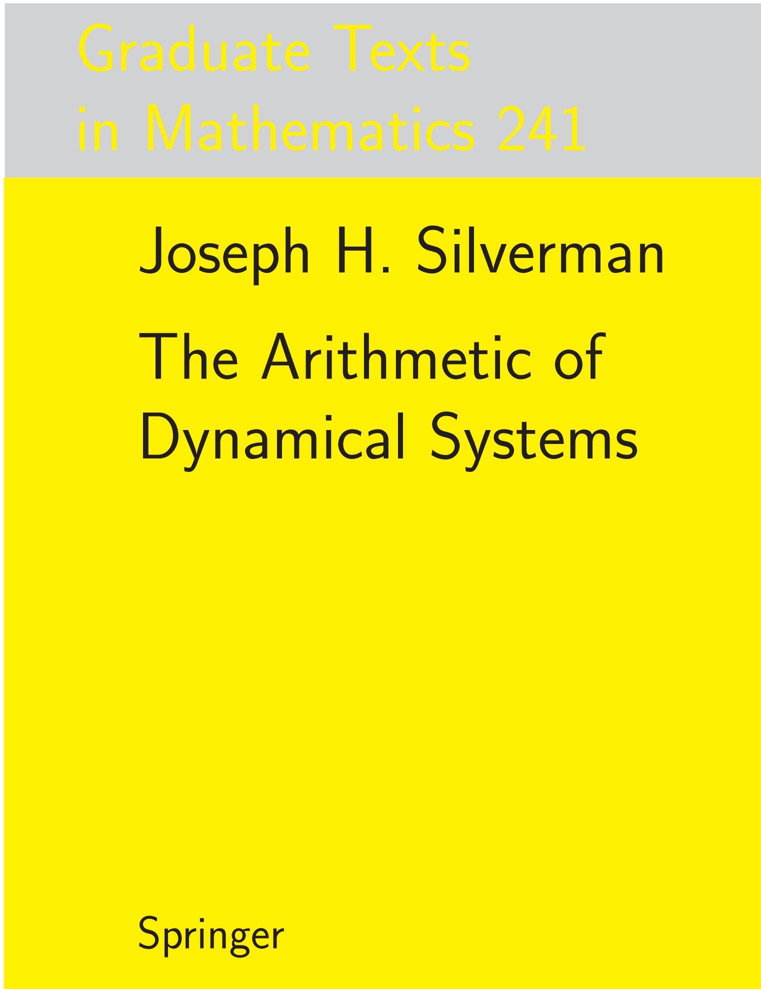
(b) $\phi(z)$ is a polynomial.

The theorem is true even in the case that $\mathrm{Aut}(\phi) \neq 1$, although the proof is more complicated.

Proof Ideas. Interpret the elements of $H^1(\mathrm{Gal}, \mathrm{PGL}_2)$ as twists of $\mathbb{P}^1$. Then use the given properties of ϕ to prove that the twists have a rational point, hence are trivial.

And In Conclusion, . . . A Blatant Advertisement

For those who are interested in learning more about arithmetic dynamics, there is now an introductory graduate textbook on the subject.



www.math.brown.edu/~jhs/ADSHome.html

Moduli Spaces in Arithmetic Dynamics

Joseph H. Silverman

Brown University

Workshop on p-adic Dynamics
Fields Institute, Toronto
Tuesday, October 28, 2008