THE MODULI SPACE OF RATIONAL FUNCTIONS OF DEGREE d

MICHELLE MANES

1. Short Introduction to Varieties

For simplicity, the whole talk is going to be over $\mathbb{C}$. This sweeps some details under the rug, but it's enough to give you an idea of what's going on.

Definition 1. *We define affine n-space to be the set of ordered n-tuples with coordinates in $\mathbb{C}$:*

$$\mathbb{A}^n = \{P = (p_1, \dots, p_n) : p_i \in \mathbb{C}\}$$

Idea: algebraic geometers wanted to investigate zeroes of polynomials.

Take an ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$. By Hilbert's basis theorem, this ring is noetherian, so the ideal is finitely generated.

Definition 2. *An (affine) algebraic set is the set of points in affine n-space where all the elements of I vanish. If I is a prime ideal, we call the algebraic set an affine variety.*

$$V(I) = \{P \in \mathbb{A}^n : f(P) = 0, \forall f \in I\}$$

Note: a point is in $V(I)$ iff $f(P) = 0$ for all the generators of I.

Notice that these algebraic sets satisfy two properties:

- Finite unions of algebraic sets are also algebraic sets. (Take products of generators of the ideals.)
- Arbitrary intersections of algebraic sets are algebraic. (Take ideal generated by union of all the generators.)

These two conditions define the closed sets of a topological space. So we can define the Zariski topology: Closed sets are algebraic sets. Open sets are the complements of algebraic sets.

For various reasons, we usually want to think about projective space, rather than affine space:

Definition 3. *We define projective n-space to be the set of ordered $n+1$-tuples with coordinates in $\mathbb{C}$, not all coordinates 0, up to equivalence: We say that $P \sim Q$ if $\exists \lambda \in \mathbb{C}^*$ such that $\lambda p_i = q_i$ for all i.*

$$\mathbb{P}^n = \{P = [p_0 : \dots : p_n] : p_i \in \mathbb{C} \ \textit{ some } p_i \neq 0\}/\mathbb{C}^*$$

One way to picture $\mathbb{P}^n$ is as the set of lines through the origin in $\mathbb{A}^{n+1}$.

It doesn't make sense to evaluate an arbitrary polynomial in $\mathbb{P}^n$; evaluate at P and λP, and get different answers. However, if the polynomial is homogeneous of degree d, then $f(\lambda P) = \lambda^d f(P)$. So it does make sense to ask if a homogeneous polynomial vanishes at a point of $\mathbb{P}^n$.

So to think about zeroes of polynomials in projective space, we need to limit ourselves to homogeneous polynomials. Otherwise, things work just like before. Take a homogeneous ideal $I \subseteq \mathbb{C}[x_0, \dots, x_n]$. (This just means generated by homogeneous polynomials... and again a finite number of them.)

Definition 4. *A projective algebraic set is the set of points in projective n-space where all the elements of I vanish. If I is a prime ideal, we call the algebraic set projective variety.*

$$V(I) = \{P \in \mathbb{P}^n : f(P) = 0, \forall f \in I\}$$

More generally, we'll use "variety" to mean a Zariski open subset of a projective variety. (So this will include affine varieties and projective varieties, but also other stuff.)

Date: July 31, 2006.

2. Introduction to Moduli Problems

The goal of a moduli problem: Find an algebraic variety whose points parameterize things that I care about. The quintessential example of this is the moduli space of elliptic curves. I'll note again that we're working over $\mathbb{C}$ which, among other nice properties, has characteristic zero. So we'll be oversimplifying a bit, but again it's good enough for our purposes.

Definition 5. *An elliptic curve will be a curve in $\mathbb{P}^2$ given by a Weierstrass equation:*

$$zy^2 = x^3 + axz^2 + bz^3$$

with the discriminant of the polynomial nonzero: $4a^3 + 27b^3 \neq 0$.

Note that if $z = 0$, we have only one point on the curve: $[0 : 1 : 0]$. Otherwise, if $z \neq 0$, we may as well assume $z = 1$. Then points on the curve will be $[x : y : 1]$ with x and y solutions of

$$y^2 = x^3 + ax + b$$

(This is familiar form of the equation for an elliptic curve.)

Note that if we take any nonzero $u \in \mathbb{C}$, we can set $y' = u^3 y$ and $x' = u^2 x$. Then we can compute:

$$\begin{aligned} y'^2 &= u^6 y^2 \\ &= u^6(x^3 + ax + b) \\ &= (u^2x)^3 + u^4 a(u^2 x) + u^6 b \\ &= x'^3 + a'x' + b' \end{aligned}$$

Two such curves are isomorphic. They have the same form of the equation and the same point at infinity; they only differ by a change of coordinates on $\mathbb{C}^2$. You can show that the only changes of variables that preserve the point $[0 : 1 : 0]$ on the curve and the form of the Weierstrass equations are the ones like this.

Definition 6. *The j-invariant of an elliptic curve given by the Weierstrass equation above is:*

$$j(E) = 1728\left(\frac{4a^3}{4a^3 + 27b^2}\right)$$

Note that $j(E)$ is a perfectly nice complex number, since we assume the curve is nonsingular. The denominator is exactly the discriminant of the polynomial, which we require to be nonzero.

Suppose two elliptic curves E and E' are related by the change of coordinates given above. Then $a' = u^4 a$ and $b' = u^6 b$. How do $j(E)$ and $j(E')$ compare? Well, we get

$$j(E') = 1728\left(\frac{4a^3u^{12}}{4a^3u^{12} + 27b^2u^{12}}\right) = j(E)$$

So if two elliptic curves are isomorphic, their j-invariants are the same. It turns out this is really iff. Also, notice that all j-values are possible. Pick any j-value you like. Then pick a value for a and solve for b. So we can define:

- "families of elliptic curves" are isomorphism classes
- moduli space of elliptic curves is then $\mathbb{A}^1$

Each j-value gives a family of elliptic curves and vice-versa. (This is a very sketchy outline of the moduli space of elliptic curves. All the details can be found in [11].)

3. Introduction to Dynamical Systems

Take $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$, the Riemann sphere. (So we'll use the coordinate $z = x/y$ rather than $[x : y]$, and we'll use $z = \infty$ for the point $[1 : 0]$.)

Definition 7. *A rational function of degree d is a map:*

$$\phi : \mathbb{P}^1 \to \mathbb{P}^1, \qquad \phi(z) = \frac{p(z)}{q(z)}, \qquad p, q \in \mathbb{C}[z], \qquad d = \deg(\phi) = \max(\deg(p), \deg(q))$$

Note: $\deg(\phi) = d$ means:

$$\phi(z) = \frac{a_d z^d + \cdots + a_0}{b_d z^d + \cdots + b_0}$$

with a_d and b_d not both 0, and $\gcd(p, q) \in \mathbb{C}^*$ (i.e. they don't have any common roots; otherwise you could cancel and get something of lower degree).

To get a dynamical system, iterate a rational function:

$$\phi(z), \phi^2(z) = \phi(\phi(z)), \phi^3(z) = \phi(\phi(\phi(z))), \ldots$$

We look at the orbit of a point:

$$[z_0] = \{z_0, \phi(z_0), \phi^2(z_0), \ldots\}$$

What kinds of things can happen?

- After some finite number of steps, you come back to where you started:
$$z_0 \mapsto \phi(z_0) \mapsto \ldots \mapsto \phi^n(z_0) \mapsto z_0$$
We say z_0 is a periodic point (of period n). Example: $\phi(z) = z^2 - 1$, $z_0 = 0$. The orbit is $0 \mapsto -1 \mapsto 0 \mapsto \ldots$.
- After some finite number of steps, you come back to some point in the orbit that's not your starting point:
$$z_0 \mapsto \phi(z_0) \mapsto \ldots \mapsto \phi^i(z_0) \mapsto \ldots \phi^n(z_0) \mapsto \phi^i(z_0)$$
We say z_0 is a preperiodic point. Example: $\phi(z) = z^2 - 1$, $z_0 = 1$. The orbit is $1 \mapsto 0 \mapsto -1 \mapsto 0 \mapsto \ldots$.
- The orbit is infinite: $z_0 \mapsto \phi(z_0) \mapsto \phi^2(z_0) \mapsto \ldots$. Examples: $\phi(z) = z^2 - 1$, $z_0 = 2$. The orbit begins $2 \mapsto 3 \mapsto 8 \mapsto 63 \mapsto \ldots$. Really, the orbit is getting sucked into a fixed point at ∞.

  A different kind of behavior can be seen in $\phi(z) = z^2 - 2.1$, $z_0 = 1.1$. The orbit begins $1.1 \mapsto -0.89 \mapsto -1.3079 \mapsto -0.389398 \mapsto -1.94837 \mapsto 1.69614 \mapsto 0.776904 \ldots$. In this case, it might be that the orbit behaves chaotically. (You can think about this in the colloquial sense of "having no predictable pattern," or you can look up the mathematical details in [2] and [3].)

Dynamicists try to classify points, regions, etc. They try to answer questions like:

- Is the orbit bounded?
- Which points have finite orbit? (They are periodic or preperiodic.)
- Which points are sucked into a cycle? Repelled away from a cycle?
- Which points have chaotic orbit?

Number theorists try to think about periodic and preperiodic points that lie in $\mathbb{Z}$, $\mathbb{Q}$, or in number fields.

4. Rat_d

The goal of a moduli problem: Find an algebraic variety whose points parameterize things that I care about. In the case of dynamics, we want to find a variety whose points parameterize rational functions of degree d. Naively, we could think like this:

$$\phi(z) = \frac{a_d z^d + \cdots + a_0}{b_d z^d + \cdots + b_0}$$

Notes:

- We have $2d + 2$ coefficients.
- Not all coefficients can be 0. (In particular, to have degree d, we need either $a_d \neq 0$ or $b_d \neq 0$.)
- For any constant c, $\frac{ca_d z^d + \cdots + ca_0}{cb_d z^d + \cdots + cb_0} = \phi(z)$.

So we can think of a point $[a_d : \ldots : a_0 : b_d : \ldots : b_0] \in \mathbb{P}^{2d+1}$. So question: do we have an equivalence: points in $\mathbb{P}^{2d+1} \leftrightarrow$ rational functions of degree d?

Well, not really. We need to add a couple of restrictions:

- If we write $\phi(z) = \frac{p(z)}{q(z)}$, we need one of $\deg(p)$ or $\deg(q)$ to be d. (So we need particular coordinates to be nonzero; $\mathbb{P}^{2d+1}$ just guarantees that *some* coordinate is nonzero.)

- We need to have no cancellation (which would give a function of lower degree). So we need p and q not to share any roots.

A useful object is the *resultant*:

$$\mathrm{Res}(p,q) = \det \begin{vmatrix} a_d & \cdots & a_0 & & \\ & a_d & \cdots & a_0 & \\ & & \vdots & & \\ & & a_d & \cdots & a_0 \\ b_d & \cdots & b_0 & & \\ & b_d & \cdots & b_0 & \\ & & \vdots & & \\ & & b_d & \cdots & b_0 \end{vmatrix}$$

Theorem 1. *$Res(p,q) = 0$ iff either:*

1. *p and q share a common root, or*
2. *both p and q have degree $< d$*

This is a pretty easy proof, just a messy calculation and induction. For details, see Appendix A in [6]. Note that this exactly takes care of the issues above, and that the resultant is a homogeneous polynomial in the coefficients of ϕ. So $V = V(\mathrm{Res}(p,q))$ is an algebraic set, a Zariski closed subset of $\mathbb{P}^{2d+1}$.

Then we have the space of rational functions of degree d: $\mathrm{Rat}_d \sim \mathbb{P}^{2d+1} \backslash V$. This is a clearly described open subset of a projective space, so it's an algebraic variety. That's what we wanted. (And in fact, people have studied this space a lot. Segal [9] showed that $\pi_1(\mathrm{Rat}_d)$ is cyclic of order $2d$, and lots of other stuff about the topology of the space.)

Note for people who know what I'm talking about: All I've really shown is that there's a variety whose complex points are in bijection with the rational maps of degree d defined over $\mathbb{C}$. Silverman showed in [12] that in fact it's a fine moduli space.

5. M_d

But: What we care about is the dynamical behavior of the function. It turns out that (lots of) different functions have identical dynamical behavior. They're isomorphic as functions, in a sense.

Remember that a change of variables on $\mathbb{C}$ gives essentially the same elliptic curve if we preserve the form of the equation. A change of variables on $\mathbb{P}^1$ gives essentially the same rational map, if we can preserve the dynamics. Recall that change of variables on $\mathbb{P}^1$ is a linear fractional transformation: $z \mapsto \frac{az+b}{cz+d}, \quad ad-bc \neq 0$. So it's an element of $\mathrm{GL}_2(\mathbb{C})$. But in fact, $z \mapsto \frac{taz+tb}{tcz+td}$ is the same LFT, so we really want to consider elements of $\mathrm{PGL}_2(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})/\mathbb{C}^*$.

It turns out that to preserve dynamics, the right change of variables is conjugation by elements of PGL_2.

Definition 8. $\phi^f = f^{-1} \circ \phi \circ f$

$$\begin{tikzcd} \mathbb{P}^1 \arrow[r, "\phi^f"] \arrow[d, "f"'] & \mathbb{P}^1 \arrow[d, "f"] \\ \mathbb{P}^1 \arrow[r, "\phi"'] & \mathbb{P}^1 \end{tikzcd}$$

Important properties:

- $\left(\phi^f\right)^n = \left(f^{-1} \circ \phi \circ f\right) \cdots \left(f^{-1} \circ \phi \circ f\right) = f^{-1} \circ \phi^n \circ f = \left(\phi^n\right)^f$
- If α is a fixed point for ϕ, then $\beta = f^{-1}(\alpha)$ is a fixed point of ϕ^f. (Similarly for other periods.)

So indeed conjugation by PGL_2 preserves dynamics. We want to consider ϕ_1 and ϕ_2 to be the same rational map if $\exists f \in \mathrm{PGL}_2$ such that $\phi_1^f = \phi_2$. This is clearly an equivalence relation, so we want to define

$M_d = \mathrm{Rat}_d/\mathrm{PGL}_2$, the moduli space of rational functions of degree d (if this even makes sense). Just as we parameterized isomorphism classes of elliptic curves, we now want to parameterize conjugacy classes of rational maps.

This is a familiar construction in topology — we create one topological space from another via quotient by a (usually finite) group action. For example $\mathbb{RP}^2 \cong S^2/\pm 1$ (identify antipodal points on the sphere to get the real projective plane). This can be problematic when you are working with an infinite group.

A weak notion of quotient, called categorical quotient, is a pair (Y, ϕ) making the following diagram commute:

$$\begin{tikzcd} G \times X \arrow[r, "g"] \arrow[d, "p_2"'] & X \arrow[d, "\phi"] \\ X \arrow[r, "\phi"'] & Y \end{tikzcd}$$

so that if you have another pair $\{Z, \psi\}$ giving a commutative diagram, you get a unique map $\chi : Y \to Z$. (Here g is the group action of G on X and p_2 is projection on the second factor. The diagram essentially says that the group action is trivial on Y, and the other condition says that Y is somehow universal in this respect.)

For example, consider $\mathbb{A}^1$ and the group action induced by $\mathbb{G}_m$ (multiplication by nonzero constants, $x \mapsto \alpha x$). You have two orbits: the nonzero constants, and the orbit of zero. The usual way to find the (categorical) quotient is to take the coordinate ring of $\mathbb{A}^1$, which is $\mathbb{C}[x]$, and then compute the ring of invariants under $\mathbb{G}_m$. The only invariants under $x \mapsto \alpha x$ are the constants. So you get the new coordinate ring $\mathbb{C}$. This is the coordinate ring of the quotient space, so the quotient space has only one point. We lose an orbit. The problem is that we want to take the invariants locally, but 0 has no neighborhood to take invariants of. Under a finite group action, we could take the intersection of finitely many neighborhoods of 0 to get a neighborhood in the quotient. But in this case, we have to take an infinite intersection, and the result is just the single point.

A stronger notion of quotient is what we want: a geometric quotient has the property that the above diagram commutes, but also that we get a bijection between points in the quotient space Y and orbits (along with some other nice properties, detailed in [8]). Silverman showed in [12] that M_d do exist as geometric quotients. We know the existence and the dimension, but not an explicit description of them, like we had with Rat_d. But M_2 is particularly nice, so we'll build it.

6. M_2

This following argument is from Milnor [6]. An almost identical argument by Silverman in [12] shows that the same result holds for any algebraically closed field, thinking of these spaces as schemes over $\mathbb{Z}$.

Claim 1. *$M_2(\mathbb{C}) \sim \mathbb{C}^2$. (In Silverman, we have the more general statement that $M_2 \sim \mathbb{A}^2$.)*

We'll prove this by finding the coordinates that determine the rational map up to conjugacy.

Claim 2. *$\phi \in Rat_2$ has three (not necessarily distinct) fixed points.*

Set $\phi(z) = z$ and solve the cubic. We get three solutions. If the degree of the resulting equation is < 3, we get fixed points at ∞ of appropriate multiplicities. Name the fixed points $z_1,\ z_2,\ z_3$.

Definition 9. *The multiplier of a fixed point: If $z_i \neq \infty$, $\lambda_i = \phi'(z_i)$. If $z_i = \infty$, choose $f \in PGL_2$ with $\beta = f^{-1}(z_i) \neq \infty$ and $\phi^f(\beta) \neq \infty$, and set $\lambda_i = \left(\phi^f\right)'(\beta)$.*

Quick computation shows that the multiplier is well defined: $\beta = f^{-1}(\alpha)$. Then

$$\begin{aligned} \left(\phi^f\right)'(\beta) &= (f^{-1} \circ \phi \circ f)(\beta) \\ &= (f^{-1})'(\phi \circ f(\beta))\phi'(f(\beta))f'(\beta) \quad \text{chain rule} \\ &= (f^{-1})'(\phi(\alpha))\phi'(\alpha)f'(f^{-1}(\alpha)) \end{aligned}$$

But we can also calculate:

$$\begin{aligned} f \circ f^{-1}(z) &= z \\ f'(f^{-1}(z))(f^{-1})'(z) &= 1 \\ f'(f^{-1}(z)) &= \frac{1}{(f^{-1})'(z)} \end{aligned}$$

Combining the two above, we get

$$\left(\phi^f\right)'(\beta) = \frac{(f^{-1})'(\phi(\alpha))}{(f^{-1})'(\alpha)}\phi'(\alpha)$$

If α is a fixed point for ϕ, then we have $\left(\phi^f\right)'(\beta) = \phi'(\alpha)$.

Why do we care about multipliers? Well, they tell you what's going on near the fixed point.

- $|\lambda_i| < 1$, then in a neighborhood of z_i the map is contracting. We have an attracting fixed point.
- $|\lambda_i| > 1$, then in a neighborhood of z_i the map is expanding. We have a repelling fixed point.
- $|\lambda_i| = 1$, we have an indifferent fixed point. Can be difficult to tell what's going on dynamically.

The multipliers form an unordered set, so we look instead at the symmetric functions of the multipliers:

$$\sigma_1 = \lambda_1 + \lambda_2 + \lambda_3, \quad \sigma_2 = \lambda_1\lambda_2 + \lambda_1\lambda_3 + \lambda_2\lambda_3 \quad \sigma_3 = \lambda_1\lambda_2\lambda_3$$

Claim 3. $\sigma_1 - 2 = \sigma_3$ *(Equivalently,* $\lambda_1\lambda_2\lambda_3 - (\lambda_1 + \lambda_2 + \lambda_3) + 2 = 0$.*)*

First assume that no $\lambda_i = 1$. If necessary, replace ϕ with ϕ^f so that ∞ is not a fixed point. Then we have a fundamental identity:

$$\sum \frac{1}{1-\lambda_i} = 1$$

We prove this by integrating $\int_{\mathbb{P}^1} \frac{dz}{z-\phi(z)} = 2\pi i \sum$ residues.

But the poles of $\frac{1}{z-\phi(z)}$ are exactly the fixed points of ϕ. To calculate the residue at z_1 for example, on the one hand we evaluate $(z - z_1)\frac{1}{z-\phi(z)}$ at z_1 to get $\frac{1}{(z_1-z_2)(z_1-z_3)}$. But on the other hand, this is exactly $\frac{1}{1-\lambda_1}$. So the integral is $2\pi i \sum \frac{1}{1-\lambda_i}$.

Now we notice that

$$\lim_{|z|\to\infty} \frac{1}{z} - \frac{1}{z-\phi(z)} = \lim_{|z|\to\infty} \frac{-\phi(z)}{z(z-\phi(z))}$$

Since we set $\phi(\infty)$ to be finite, this limit is 0. So we have:

$$\begin{aligned} \int_{\mathbb{P}^1} \frac{dz}{z-\phi(z)} &= \lim_{R\to\infty} \int_{|z|=R} \frac{dz}{z-\phi(z)} \\ &= \lim_{R\to\infty} \int_{|z|=R} \frac{dz}{z} \\ &= 2\pi i \end{aligned}$$

And we get the desired result.

Given $\sum \frac{1}{1-\lambda_i} = 1$, we simply get a common denominator and simplify to get the desired result:

$$\begin{aligned} \frac{1}{1-\lambda_1} + \frac{1}{1-\lambda_2} + \frac{1}{1-\lambda_3} &= 1 \\ (1-\lambda_2)(1-\lambda_3) + (1-\lambda_1)(1-\lambda_3) + (1-\lambda_1)(1-\lambda_2) &= (1-\lambda_1)(1-\lambda_2)(1-\lambda_3) \end{aligned}$$

Claim 4. *$\lambda_i = 1$ iff z_i is a multiple fixed point, so that $z_i = z_j$ for some $i \neq j$.*

Write $\phi(z) - z = (z-z_1)(z-z_2)(z-z_3)$, so $\phi'(z) - 1 = (z-z_2)(z-z_3) + (z-z_1)(z-z_3) + (z-z_1)(z-z_2)$. We get $\phi'(z_i) = 0$ iff $z_i = z_j$. So if $\lambda_1 = 1$ then also WLOG $\lambda_2 = 1$, and the equation becomes $\lambda_3 - \lambda_3 - 2 + 2 = 0$, which holds for any value of λ_3.

Theorem 2. *The conjugacy class of ϕ is determined by $\{\lambda_1, \lambda_2, \lambda_3\}$.*

First suppose ϕ has at least two fixed points. Conjugate by f so that the fixed points are at 0 and ∞. Then we must have $\phi(z) = z\left(\frac{az+b}{cz+d}\right)$. Because we have $\deg(\phi) = 2$, we know $a \neq 0$, $d \neq 0$, and $ad - bc \neq 0$.

We can multiply by a constant to get $d = 1$. Then conjugate by $z \mapsto a^{-1}z$ to get $\phi(z) = z\left(\frac{z+b}{cz+1}\right)$ with $1 - bc \neq 0$.

It's easy to check that $\phi'(0) = b$ and the multiplier at ∞ is c. (Conjugate by $\frac{1}{z}$.) We already saw that the set of multipliers are preserved under conjugation by PGL_2. So any rational map with multipliers b and c is conjugate to this ϕ.

Now suppose there's only one fixed point. We can conjugate ϕ so as to move that fixed point to ∞, and we can also conjugate so that $\phi^{-1}(\infty) = \{0, \infty\}$. (The multiplier is not 0, so ∞ is not a critical point. This means we have another point in the preimage.)

So $\phi(z) = \frac{p(z)}{z}$ for some quadratic polynomial $p(z)$. Then $\phi(z) - z = \frac{p(z)-z^2}{z} \neq 0$ for any finite z. (No fixed points in $\mathbb{C}$.) That means that $p(z) - z^2$ is a constant, so $p(z) = z^2 + c$.

Then $\phi(z) = \frac{z^2+c}{z} = z + \frac{c}{z}$. Conjugate by $f(z) = \sqrt{c}z$ to get $\phi(z) = z + \frac{1}{z}$. Then $\lambda_1 = \lambda_2 = \lambda_3 = 1$. We know this happens only when there is just one fixed point. So again, the conjugacy class is determined by the multipliers.

So we have $\phi(z) \in \mathrm{Rat}_2$ gives multipliers $\{\lambda_1, \lambda_2, \lambda_3\}$ (unordered), which gives the symmetric functions (σ_1, σ_2). So M_d is some subset of $\mathbb{A}^2$. We just need to show we get all of it.

But that's clear: We can get any pair $\{\lambda_1, \lambda_2\}$ with one of the two normal forms, and λ_3 is determined by this. On the other hand, choose any (σ_1, σ_2). The multipliers are determined as roots of

$$x^3 - \sigma_1 x^2 + \sigma_2 x - (\sigma_1 - 2)$$

So we get all of $\mathbb{A}^2$.

What we've shown is that there's a bijection of points between $M_2(\mathbb{C})$ and $\mathbb{C}^2$. We have a bijection of sets

$$(\sigma_1, \sigma_2) : M_2(\mathbb{C}) \to \mathbb{C}^2$$

However, we don't know that this map is an isomorphism of varieties.

Definition 10. *A rational map ϕ of varieties is regular at a point P if $\exists f, g \in \mathbb{C}[x]$ such that in a neighborhood of P, $\phi = \frac{f}{g}$ with $g(P) \neq 0$.*

To have an isomorphism, we need to have maps that are regular at every point, bijective, bicontinuous. Example of where we don't get regularity:

$\phi : \mathbb{A}^1 \to \mathbb{A}^2$ defined by $t \mapsto (t^2, t^3)$. So this function is bijective and bicontinuous, but in a neighborhood of 0, there is no way to write the inverse as a regular function. This captures something important about the two varieties. The cubic curve has a singularity at $(0, 0)$, and the affine line is nonsingular.

In our current case, note that the action of PGL_2 is not free. $z \mapsto -z$ acts trivially on every odd function (e.g. $\phi(z) = z + \frac{1}{z}$). We might expect singularities to crop up at these points, and the construction we've done so far wouldn't show them.

In the case of $\mathbb{C}$, we use the fact that PGL_2 is a reductive group, so we get a good quotient. In the more general case, Silverman [12] proves the following theorem:

Theorem 3. *Let $F : X \to Y$ be a morphism of schemes over $\mathbb{Z}$. Suppose that the following four conditions are true:*

1. *X is an integral scheme. (All rings $O_X(U)$ are integral domains. Equivalent to reduced and irreducible.)*
2. *Y is an integral normal scheme that is dominant over $\mathbb{Z}$. (Normal means all local rings are integrally closed domains. Dominant means image is dense.)*
3. *F is a finite morphism. (Cover Y by $V_i = SpecB_i$ such that $F^{-1}(V_i) = SpecA_i$ and A_i is finitely generated as an B_i module.)*
4. *F induces a bijection on geometric points.*

Then F is an isomorphism.

He then shows that the four conditions hold in this situation.

7. M_d for $d > 2$

So we have a very nice result for M_2. We would like to extend it in some way to M_d for $d > 2$. Here's the idea of a setup:

For any $n \geq 1$, we can define points of period n by solutions to $\phi^n(z) = z$. Just as before, we can define multipliers for a cycle. Take any point z_i of period n. Define $\lambda_i^{(n)} = (\phi^n)'(z_0)$, and make a suitable change of coordinate to define it for $z_i = \infty$. Multipliers must be the same for every point in a cycle (by the chain rule). Again, multipliers give us an unordered set $\{\lambda_i^{(n)}\}$, so we look instead at symmetric functions of the multipliers: $\{\sigma_1^{(n)}, \ldots, \sigma_N^{(n)}\}$. (Here N is the number of n-cylces, so the number of multipliers we get.)

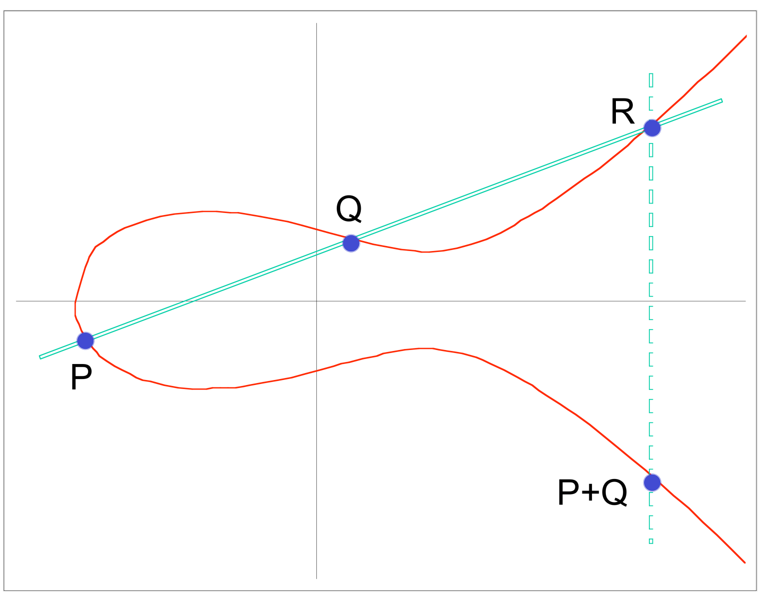
In [12] Silverman shows that these are in fact global sections of $\mathcal{O}_{\mathrm{Rat}_d}$. We showed for $\sigma_i^{(1)}$ that they are invariant under PGL_2 action, and the proof is much the same for other $\sigma_i^{(n)}$. So they are in fact global sections of $\mathcal{O}_{M_d}$. So we can use them to define a map

$$\tau^{(n)} : M_d \to \mathbb{A}^m, \quad \phi \mapsto (\sigma_1^{(1)}(\phi), \sigma_2^{(1)}(\phi), \sigma_3^{(1)}(\phi), \sigma_1^{(2)}(\phi) \ldots, \sigma_N^{(n)}(\phi))$$

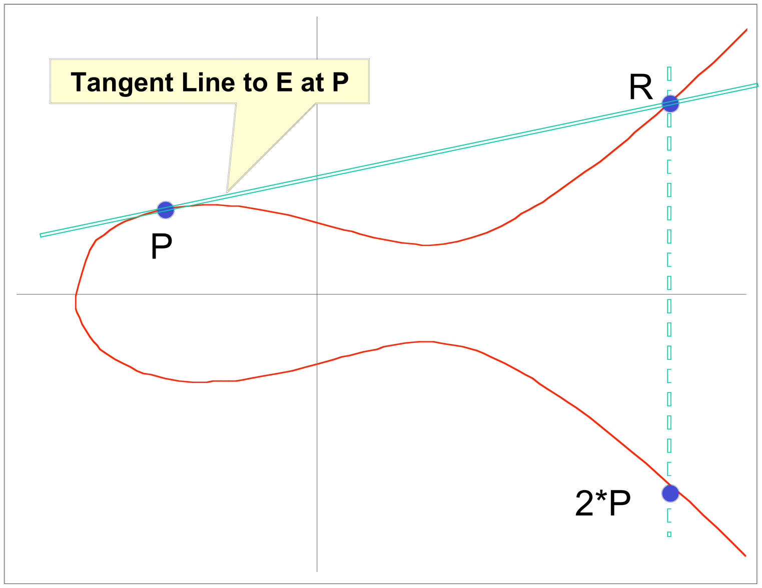
(We use as coordinates the symmetric functions of multipliers for every j-cycle up to period n.) The hope would be that if we choose n sufficiently large (take multipliers for periodic points of high enough period), we could get an embedding. For example, we showed that for M_2, $\tau^{(1)}$ gives an embedding. It turns out that for infinitely many $d = \deg(\phi)$ that won't be possible.

We need to come back to elliptic curves to look at what goes wrong. (For details on just about everything that follows, see [10] and [11].) One thing that's special about elliptic curves is that their points can be given a group structure. That is, we can define what it means to add two points on a elliptic curve. When we write the equation in Weierstrass form as we did before, the "identity" is the point at infinity. To add two points P and Q on your curve, draw the line connecting them, and find its third intersection with the curve. Then draw the vertical line through this point (i.e. the line through that point and the point at infinity). The other intersection of that line with the curve gives the point $P + Q$.

(The following pictures were shamelessly stolen from Joe Silverman's talk "The Ubiquity of Elliptic Curves," available on his website at http://math.brown.edu/~jhs.)



So we can extend this to multiply a point by 2: To get $2P$, you draw the tangent line through P, find the other intersection with the curve, then draw the vertical line through that point. To get nP for any n, iterate the process.



Since we have equations for our curves, all of this can be made algebraic. That is, we can write equations for multiplying points by 2. Let $P = (x, y)$ be a point on our curve. Then

$$x([2]P) = \frac{x^4 - 2ax^2 - 4bx + a^2}{4x^3 + 4ax + 4b}$$

We can find $y([2]P)$ by solving the Weierstrass equation (we'll get two answers, and we'll need to determine the sign based on the original point P).

Also note that in our Weierstrass equations, if (x, y) is on the curve, so is $(x, -y)$ (and in fact, this point is exactly the inverse of (x, y) under the group law). So we can create a 2-to-1 map $E \to \mathbb{P}^1$ by $(x, y) \mapsto x$. Then we can define a rational map $\phi_{E,m} : \mathbb{P}^1 \to \mathbb{P}^1$ making the following diagram commute:

$$\begin{tikzcd}
E \arrow[r, "{[m]}"] \arrow[d, "x"'] & E \arrow[d, "x"] \\
\mathbb{P}^1 \arrow[r, "\phi_{E,m}"'] & \mathbb{P}^1
\end{tikzcd}$$

If you know a little about elliptic curves, you know that the multiplication-by-m map has degree m^2. So $\deg(\phi_{E,m}) = m^2$. This map (called a Lattès map) creates our problem.

Claim 5. *The multipliers of $\phi_{E,m}$ (and iterates) are independent of E. But non-isomorphic elliptic curves give nonconjugate maps $\phi_{E,m}$.*

First, we'll prove the multipliers are independent of E. The easiest way to see this is if you know that a complex elliptic curve is a complex torus. That is, it's $\mathbb{C}/\Lambda$ for some lattice Λ. In this case, the multiplication by m map is really just multiplying a point in the complex plane z by m. The map to $\mathbb{P}^1$ sends all of the points of Λ to the point at infinity, and is everywhere else defined by the Weierstrass $\wp$ function: $z \mapsto [\wp(z), \wp'(z), 1]$.

So we have a commutative diagram:

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{z\mapsto mz} & \mathbb{C}/\Lambda \\ \Big\downarrow{\scriptstyle \wp(z)} & & \Big\downarrow{\scriptstyle \wp(z)} \\ \mathbb{P}^1 & \xrightarrow[\phi_{E,m}]{} & \mathbb{P}^1 \end{array}$$

If $w = \wp(z)$ is a fixed point of ϕ, using the commutativity of the diagram, we get $\phi(\wp(z)) = \wp(mz) = \wp(z)$. Since modulo Λ each point has only two preimages under $\wp$, we must have $mz \equiv \pm z \pmod{\Lambda}$.

First we compute the multiplier at some fixed point $w = \wp(z)$:

$$\begin{aligned} (\phi(\wp(z))' &= (\wp(mz))' \\ \phi'(\wp(z))\wp'(z) &= m\wp'(mz) \\ \phi'(\wp(z)) &= m\frac{\wp'(mz)}{\wp'(z)} \end{aligned}$$

Now, we know that $\wp'$ is an odd elliptic function, and that $mz \equiv \pm z \pmod{\Lambda}$. These two facts together tell us that $\frac{\wp'(mz)}{\wp'(z)} = \pm 1$. (Another way to see this: The points $(\wp(z), \wp'(z))$ and $(\wp(mz), \wp'(mz))$ are both on the elliptic curve, and they have the same x-coordinate. So they are either the same point or the y-coordinates are negatives of each other, since points on the elliptic curve are of the form $(x, \pm\sqrt{f(x)})$ with $y^2 = f(x)$ the defining equation of the curve.)

So even though the functions $\wp$ and ϕ depend on the particular lattice we choose, the multipliers are all $\pm m$.

Now, suppose that we have another elliptic curve E', and that the two induced maps $\phi_{E,m}$ and $\phi_{E',m}$ are conjugate. That is, $\exists f \in \mathrm{PGL}_2$ so that $\phi^f_{E,m} = \phi_{E',m}$. (Note: the m's must be the same because the induced maps both have degree m^2.) Then we have this commutative diagram:

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

We know (see for example [10]) that we may write the equation for E (over $\mathbb{C}$) in the form $y^2 = x(x-1)(x-\lambda)$, and similarly we may write the equation for E' as $y^2 = x(x-1)(x-\lambda')$. Calculation of the j-invariant in terms of λ shows that $E \cong E'$ iff $\lambda \in \{\lambda', \frac{1}{\lambda'}, 1-\lambda', \frac{1}{1-\lambda'}, \frac{\lambda'}{1-\lambda'}, \frac{1-\lambda'}{\lambda'}\}$. We will show that this must be the case if the maps $\phi_{E,m}$ and $\phi_{E',m}$ are conjugate.

Note that all of the maps in the diagram above are surjective. Following Milnor in [7], we let V_F be the set of critical values of a map F (A "critical value" is simply the image of a critical point.)

By commutativity of the diagram, $z_0 \in \mathbb{P}^1$ is a critical value of x iff either z_0 is also a critical value of $\phi_{E,m}$, or there is a point $z_1 \in \phi^{-1}_{E,m}(z_0)$ such that z_1 is a critical value of x. In other words: $V_x = V_{\phi_{E,m}} \cup \phi_{E,m}(V_x)$.

Inductively, then, we have:

$$V_x = V_{\phi_{E,m}} \cup \phi_{E,m}(V_{\phi_{E,m}}) \cup \phi_{E,m}^2(V_{\phi_{E,m}}) \cup \cdots$$

By the same argument, we have:

$$V_{x'} = V_{\phi_{E',m}} \cup \phi_{E',m}(V_{\phi_{E',m}}) \cup \phi_{E',m}^2(V_{\phi_{E',m}}) \cup \cdots$$

Following Milnor's in [7], we let V_F be the set of critical values of a map F and $P_F = V_F \cup F(V_F) \cup F^2(V_F) \cup \cdots$. (A "critical value" is simply the image of a critical point.) Lemma 3.4 in [7] shows that $V_x = P_\phi$; the proof is sketched below for this specific context.

Note that all of the maps in the diagram above are surjective, and that the multiplication-by-m map has no critical points. By commutativity of the diagram and these facts, $z_0 \in \mathbb{P}^1$ is a critical value of x iff either z_0 is also a critical value of $\phi_{E,m}$, or there is a point $z_1 \in \phi_{E,m}^{-1}(z_0)$ such that z_1 is a critical value of x. In other words: $V_x = V_{\phi_{E,m}} \cup \phi_{E,m}(V_x)$. Inductively, then, $\phi^n(V_{\phi_{E,m}}) \subset V_x$. So we have one containment: $V_x \supseteq P_{\phi_{E,m}}$.

Suppose now there is some critical point τ_0 of x such that $x(\tau_0) = z_0 \notin P_{\phi_{E,m}}$. It's clear from the definition that $\phi_{E,m}(P_{\phi_{E,m}}) \subseteq P_{\phi_{E,m}}$, so remarks from the paragraph above lead us to conclude that every preimage of τ_0 is also a critical point of x, and also has image outside $P_{\phi_{E,m}}$. There are infinitely many preimages of τ_0 under $[m]$ and its iterates, and all of these images would have to share this property. However, x can have only finitely many critical points, so this contradiction proves the other containment. We have, then, $V_x = P_{\phi_{E,m}}$, and by the same argument $V_{x'} = P_{\phi_{E',m}}$.

But by conjugacy of the maps, if α is a critical value of $\phi_{E,m}$, then $f^{-1}(\alpha)$ is a critical value of $\phi_{E',m}$. So we have:

$$V_{x'} = f^{-1}\left(V_{\phi_{E,m}}\right) \cup \phi_{E',m} f^{-1}\left(V_{\phi_{E,m}}\right) \cup \phi_{E',m}^2 f^{-1}\left(V_{\phi_{E,m}}\right) \cup \cdots$$

By conjugacy of the maps, we have $\phi_{E',m}^n f^{-1} = f^{-1}\phi_{E,m}^n$ for every n, so we get:

$$V_{x'} = f^{-1}\left(V_{\phi_{E,m}}\right) \cup f^{-1}\left(\phi_{E,m}(V_{\phi_{E,m}})\right) \cup f^{-1}\left(\phi_{E',m}^2(V_{\phi_{E,m}})\right) \cup \cdots = f^{-1}(V_x)$$

By construction, we have $V_x = \{0, 1, \infty, \lambda\}$ and $V_{x'} = \{0, 1, \infty, \lambda'\}$. Suppose we know that for $f \in \mathrm{PGL}_2$ we have $f(\alpha) = 0$, $f(\beta) = 1$, $f(\gamma) = \infty$, and $f(\delta) = \lambda$. We see that

$$f(z) = \frac{z-\alpha}{z-\gamma}\frac{\beta-\gamma}{\beta-\alpha} \Rightarrow f(\delta) = \lambda = \frac{\delta-\alpha}{\delta-\gamma}\frac{\beta-\gamma}{\beta-\alpha}$$

Running through the four possible values in $V_{x'}$, we see that we get $\lambda \in \{\lambda', \frac{1}{\lambda'}, 1-\lambda', \frac{1}{1-\lambda'}, \frac{\lambda}{1-\lambda'}, \frac{1-\lambda'}{\lambda}\}$.

This result says that in M_{m^2}, we have a whole line of of rational maps (the j-line of elliptic curves) which gets collapsed to a single point by any map $\tau^{(n)}$.

The best we can do (so far) is a result of McMullen [5]:

Theorem 4. *For sufficiently large n, the map $\tau^{(n)} : M_d(\mathbb{C}) \to \mathbb{A}^m(\mathbb{C})$ is finite-to-one except when d is a square, in which case it is finite-to-one away from the Lattès locus.*

References

[1] Alan Beardon. *Iteration of Rational Functions*, volume 132 of *Grad. Texts in Math.*. Springer-Verlag., 1991.
[2] Robert Devaney. *A First Course in Chaotic Dynamical Systems*. Addison Wesley., 1992.
[3] Robert Devaney. *An Introduction to Chaotic Dynamical Systems*. Westview., 2003.
[4] Robin Hartshorne. *Algebraic Geometry*, volume 52 of *Grad. Texts in Math.*. Springer-Verlag., 1977.
[5] C. McMullen. Families of rational maps and iterative root-finding algorithms. *Experiment. Math.*, 2, 1993.
[6] J. Milnor. Geometry and dynamics of quadratic rational maps. *Experiment. Math.*, 2, 1993.
[7] J. Milnor. On lattès maps. *IMS preprint*, 2004. Available at http://www.math.sunysb.edu/~jack/PREPRINTS/.
[8] David Mumford. *Geometric Invariant Theory*. Springer-Verlag., 1965.
[9] Graeme Segal. The topology of spaces of rational functions. *Acta Math.*, 26, 1977.
[10] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Grad. Texts in Math.* Springer-Verlag., 1986.
[11] Joseph H. Silverman. *Advanced Topics in the The Arithmetic of Elliptic Curves*, volume 151 of *Grad. Texts in Math.* Springer-Verlag., 1994.
[12] Joseph H. Silverman. The space of rational maps on $\mathbb{P}^1$. *Duke Mathematical Journal*, 94(1), 1998.