

The functional equation  $f(P) = g(Q)$  in dynamics,  
number theory, analysis and algebraic geometry

Michael Zieve

University of Michigan

April 25, 2013

Joint work with Alex Carney, Thao Do, Jared Hallett, Ruthi Hortsch,  
Xiangyi Huang, Yuwei Jiang, Qingyun Sun, Ben Weiss, Elliot Wells,  
Susan Xia

# The functional equation $f(P) = g(Q)$

Instances of this equation have been studied for centuries:

- Abel, 1826:  $(X + 1) \circ P = P \circ Q$
- Schröder 1871, ..., Yoccoz 1995:  $\lambda X \circ P = P \circ Q$
- Fatou, Julia, Ritt, 1920's:  $f \circ g = g \circ f$  with  $f, g \in \mathbb{C}(X)$
- and many more.

We know all *polynomials*  $f, P, g, Q$  such that  $f \circ P = g \circ Q$  (Ritt, 1922).

But we aren't close to knowing all solutions in rational functions: the most general published result is if  $f, g$  are polynomials and  $P, Q \in \mathbb{C}[X, 1/X]$  are Laurent polynomials (Pakovich, Z 2007).

Today I'll present all solutions when  $f, g$  are polynomials and  $P, Q$  are rational functions (or more generally, meromorphic functions on  $\mathbb{C}$ ), and give several consequences.

# The functional equation $f(P) = g(Q)$

Instances of this equation have been studied for centuries:

- **Abel, 1826:**  $(X + 1) \circ P = P \circ Q$
- **Schröder 1871, ..., Yoccoz 1995:**  $\lambda X \circ P = P \circ Q$
- **Fatou, Julia, Ritt, 1920's:**  $f \circ g = g \circ f$  with  $f, g \in \mathbb{C}(X)$
- and many more.

We know all *polynomials*  $f, P, g, Q$  such that  $f \circ P = g \circ Q$  (**Ritt, 1922**).

But we aren't close to knowing all solutions in rational functions: the most general published result is if  $f, g$  are polynomials and  $P, Q \in \mathbb{C}[X, 1/X]$  are Laurent polynomials (**Pakovich, Z 2007**).

Today I'll present all solutions when  $f, g$  are polynomials and  $P, Q$  are rational functions (or more generally, meromorphic functions on  $\mathbb{C}$ ), and give several consequences.

# The functional equation $f(P) = g(Q)$

Instances of this equation have been studied for centuries:

- **Abel, 1826:**  $(X + 1) \circ P = P \circ Q$
- **Schröder 1871, ..., Yoccoz 1995:**  $\lambda X \circ P = P \circ Q$
- **Fatou, Julia, Ritt, 1920's:**  $f \circ g = g \circ f$  with  $f, g \in \mathbb{C}(X)$
- and many more.

We know all *polynomials*  $f, P, g, Q$  such that  $f \circ P = g \circ Q$  (**Ritt, 1922**).

But we aren't close to knowing all solutions in rational functions: the most general published result is if  $f, g$  are polynomials and  $P, Q \in \mathbb{C}[X, 1/X]$  are Laurent polynomials (**Pakovich, Z 2007**).

Today I'll present all solutions when  $f, g$  are polynomials and  $P, Q$  are rational functions (or more generally, meromorphic functions on  $\mathbb{C}$ ), and give several consequences.

# The functional equation $f(P) = g(Q)$

Instances of this equation have been studied for centuries:

- **Abel, 1826:**  $(X + 1) \circ P = P \circ Q$
- **Schröder 1871, ..., Yoccoz 1995:**  $\lambda X \circ P = P \circ Q$
- **Fatou, Julia, Ritt, 1920's:**  $f \circ g = g \circ f$  with  $f, g \in \mathbb{C}(X)$
- and many more.

We know all *polynomials*  $f, P, g, Q$  such that  $f \circ P = g \circ Q$  (**Ritt, 1922**).

But we aren't close to knowing all solutions in rational functions: the most general published result is if  $f, g$  are polynomials and  $P, Q \in \mathbb{C}[X, 1/X]$  are Laurent polynomials (**Pakovich, Z 2007**).

Today I'll present all solutions when  $f, g$  are polynomials and  $P, Q$  are rational functions (or more generally, meromorphic functions on  $\mathbb{C}$ ), and give several consequences.

# The functional equation $f(P) = g(Q)$

Instances of this equation have been studied for centuries:

- **Abel, 1826:**  $(X + 1) \circ P = P \circ Q$
- **Schröder 1871, ..., Yoccoz 1995:**  $\lambda X \circ P = P \circ Q$
- **Fatou, Julia, Ritt, 1920's:**  $f \circ g = g \circ f$  with  $f, g \in \mathbb{C}(X)$
- and many more.

We know all *polynomials*  $f, P, g, Q$  such that  $f \circ P = g \circ Q$  (**Ritt, 1922**).

But we aren't close to knowing all solutions in rational functions: the most general published result is if  $f, g$  are polynomials and  $P, Q \in \mathbb{C}[X, 1/X]$  are Laurent polynomials (**Pakovich, Z 2007**).

Today I'll present all solutions when  $f, g$  are polynomials and  $P, Q$  are rational functions (or more generally, meromorphic functions on  $\mathbb{C}$ ), and give several consequences.

# The functional equation $f(P) = g(Q)$

Instances of this equation have been studied for centuries:

- **Abel, 1826:**  $(X + 1) \circ P = P \circ Q$
- **Schröder 1871, ..., Yoccoz 1995:**  $\lambda X \circ P = P \circ Q$
- **Fatou, Julia, Ritt, 1920's:**  $f \circ g = g \circ f$  with  $f, g \in \mathbb{C}(X)$
- and many more.

We know all *polynomials*  $f, P, g, Q$  such that  $f \circ P = g \circ Q$  (**Ritt, 1922**).

But we aren't close to knowing all solutions in rational functions: the most general published result is if  $f, g$  are polynomials and  $P, Q \in \mathbb{C}[X, 1/X]$  are Laurent polynomials (**Pakovich, Z 2007**).

Today I'll present all solutions when  $f, g$  are polynomials and  $P, Q$  are rational functions (or more generally, meromorphic functions on  $\mathbb{C}$ ), and give several consequences.

# The functional equation $f(P) = g(Q)$

Instances of this equation have been studied for centuries:

- **Abel, 1826:**  $(X + 1) \circ P = P \circ Q$
- **Schröder 1871, ..., Yoccoz 1995:**  $\lambda X \circ P = P \circ Q$
- **Fatou, Julia, Ritt, 1920's:**  $f \circ g = g \circ f$  with  $f, g \in \mathbb{C}(X)$
- and many more.

We know all *polynomials*  $f, P, g, Q$  such that  $f \circ P = g \circ Q$  (**Ritt, 1922**).

But we aren't close to knowing all solutions in rational functions: the most general published result is if  $f, g$  are polynomials and  $P, Q \in \mathbb{C}[X, 1/X]$  are Laurent polynomials (**Pakovich, Z 2007**).

Today I'll present all solutions when  $f, g$  are polynomials and  $P, Q$  are rational functions (or more generally, meromorphic functions on  $\mathbb{C}$ ), and give several consequences.



# The functional equation $f(P) = g(Q)$

Instances of this equation have been studied for centuries:

- **Abel, 1826:**  $(X + 1) \circ P = P \circ Q$
- **Schröder 1871, ..., Yoccoz 1995:**  $\lambda X \circ P = P \circ Q$
- **Fatou, Julia, Ritt, 1920's:**  $f \circ g = g \circ f$  with  $f, g \in \mathbb{C}(X)$
- and many more.

We know all *polynomials*  $f, P, g, Q$  such that  $f \circ P = g \circ Q$  (**Ritt, 1922**).

But we aren't close to knowing all solutions in rational functions: the most general published result is if  $f, g$  are polynomials and  $P, Q \in \mathbb{C}[X, 1/X]$  are Laurent polynomials (**Pakovich, Z 2007**).

Today I'll present all solutions when  $f, g$  are polynomials and  $P, Q$  are rational functions (or more generally, meromorphic functions on  $\mathbb{C}$ ), and give several consequences.

## A dynamics result

**Theorem (Ghioca–Tucker–Z, 2008 & 2012):** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)) \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Proof sketch:

- Writing  $f^k(X)$  for the  $k$ -th iterate of  $f$ , we have  $f^k(\alpha) = g^\ell(\beta)$  for infinitely many pairs  $(k, \ell)$ .
- For any  $n, m$ , the equation  $f^m(X) = g^n(Y)$  has infinitely many solutions  $X = f^{k-m}(\alpha)$ ,  $Y = g^{\ell-n}(\beta)$ .
- Every  $f^i(\alpha)$  and  $g^j(\beta)$  lies in the ring  $R$  generated by  $\alpha, \beta$  and the coefficients of  $f$  and  $g$ .
- Hence (Siegel, 1929; Lang, 1960) there are nonconstant Laurent polynomials  $P, Q \in \mathbb{C}[X, 1/X]$  such that  $f^m \circ P = g^n \circ Q$ .
- Solve this for each  $m, n$ , then piece together the solutions.

Summary: From dynamics to number theory to  $F(P) = G(Q)$  to QED.

## A dynamics result

**Theorem (Ghioca–Tucker–Z, 2008 & 2012):** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)) \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Proof sketch:

- Writing  $f^k(X)$  for the  $k$ -th iterate of  $f$ , we have  $f^k(\alpha) = g^\ell(\beta)$  for infinitely many pairs  $(k, \ell)$ .
- For any  $n, m$ , the equation  $f^m(X) = g^n(Y)$  has infinitely many solutions  $X = f^{k-m}(\alpha)$ ,  $Y = g^{\ell-n}(\beta)$ .
- Every  $f^i(\alpha)$  and  $g^j(\beta)$  lies in the ring  $R$  generated by  $\alpha, \beta$  and the coefficients of  $f$  and  $g$ .
- Hence (Siegel, 1929; Lang, 1960) there are nonconstant Laurent polynomials  $P, Q \in \mathbb{C}[X, 1/X]$  such that  $f^m \circ P = g^n \circ Q$ .
- Solve this for each  $m, n$ , then piece together the solutions.

Summary: From dynamics to number theory to  $F(P) = G(Q)$  to QED.

## A dynamics result

**Theorem (Ghioca–Tucker–Z, 2008 & 2012):** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)) \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Proof sketch:

- Writing  $f^k(X)$  for the  $k$ -th iterate of  $f$ , we have  $f^k(\alpha) = g^\ell(\beta)$  for infinitely many pairs  $(k, \ell)$ .
- For any  $n, m$ , the equation  $f^m(X) = g^n(Y)$  has infinitely many solutions  $X = f^{k-m}(\alpha)$ ,  $Y = g^{\ell-n}(\beta)$ .
- Every  $f^i(\alpha)$  and  $g^j(\beta)$  lies in the ring  $R$  generated by  $\alpha, \beta$  and the coefficients of  $f$  and  $g$ .
- Hence (Siegel, 1929; Lang, 1960) there are nonconstant Laurent polynomials  $P, Q \in \mathbb{C}[X, 1/X]$  such that  $f^m \circ P = g^n \circ Q$ .
- Solve this for each  $m, n$ , then piece together the solutions.

Summary: From dynamics to number theory to  $F(P) = G(Q)$  to QED.

## A dynamics result

**Theorem (Ghioca–Tucker–Z, 2008 & 2012):** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)) \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Proof sketch:

- Writing  $f^k(X)$  for the  $k$ -th iterate of  $f$ , we have  $f^k(\alpha) = g^\ell(\beta)$  for infinitely many pairs  $(k, \ell)$ .
- For any  $n, m$ , the equation  $f^m(X) = g^n(Y)$  has infinitely many solutions  $X = f^{k-m}(\alpha)$ ,  $Y = g^{\ell-n}(\beta)$ .
- Every  $f^i(\alpha)$  and  $g^j(\beta)$  lies in the ring  $R$  generated by  $\alpha, \beta$  and the coefficients of  $f$  and  $g$ .
- Hence (Siegel, 1929; Lang, 1960) there are nonconstant Laurent polynomials  $P, Q \in \mathbb{C}[X, 1/X]$  such that  $f^m \circ P = g^n \circ Q$ .
- Solve this for each  $m, n$ , then piece together the solutions.

Summary: From dynamics to number theory to  $F(P) = G(Q)$  to QED.

## A dynamics result

**Theorem (Ghioca–Tucker–Z, 2008 & 2012):** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)) \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Proof sketch:

- Writing  $f^k(X)$  for the  $k$ -th iterate of  $f$ , we have  $f^k(\alpha) = g^\ell(\beta)$  for infinitely many pairs  $(k, \ell)$ .
- For any  $n, m$ , the equation  $f^m(X) = g^n(Y)$  has infinitely many solutions  $X = f^{k-m}(\alpha)$ ,  $Y = g^{\ell-n}(\beta)$ .
- Every  $f^i(\alpha)$  and  $g^j(\beta)$  lies in the ring  $R$  generated by  $\alpha, \beta$  and the coefficients of  $f$  and  $g$ .
- Hence (Siegel, 1929; Lang, 1960) there are nonconstant Laurent polynomials  $P, Q \in \mathbb{C}[X, 1/X]$  such that  $f^m \circ P = g^n \circ Q$ .
- Solve this for each  $m, n$ , then piece together the solutions.

Summary: From dynamics to number theory to  $F(P) = G(Q)$  to QED.

## A dynamics result

**Theorem (Ghioca–Tucker–Z, 2008 & 2012):** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)) \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Proof sketch:

- Writing  $f^k(X)$  for the  $k$ -th iterate of  $f$ , we have  $f^k(\alpha) = g^\ell(\beta)$  for infinitely many pairs  $(k, \ell)$ .
- For any  $n, m$ , the equation  $f^m(X) = g^n(Y)$  has infinitely many solutions  $X = f^{k-m}(\alpha)$ ,  $Y = g^{\ell-n}(\beta)$ .
- Every  $f^i(\alpha)$  and  $g^j(\beta)$  lies in the ring  $R$  generated by  $\alpha, \beta$  and the coefficients of  $f$  and  $g$ .
- Hence (Siegel, 1929; Lang, 1960) there are nonconstant Laurent polynomials  $P, Q \in \mathbb{C}[X, 1/X]$  such that  $f^m \circ P = g^n \circ Q$ .
- Solve this for each  $m, n$ , then piece together the solutions.

Summary: From dynamics to number theory to  $F(P) = G(Q)$  to QED.

## A dynamics result

**Theorem (Ghioca–Tucker–Z, 2008 & 2012):** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)) \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Proof sketch:

- Writing  $f^k(X)$  for the  $k$ -th iterate of  $f$ , we have  $f^k(\alpha) = g^\ell(\beta)$  for infinitely many pairs  $(k, \ell)$ .
- For any  $n, m$ , the equation  $f^m(X) = g^n(Y)$  has infinitely many solutions  $X = f^{k-m}(\alpha)$ ,  $Y = g^{\ell-n}(\beta)$ .
- Every  $f^i(\alpha)$  and  $g^j(\beta)$  lies in the ring  $R$  generated by  $\alpha, \beta$  and the coefficients of  $f$  and  $g$ .
- Hence (Siegel, 1929; Lang, 1960) there are nonconstant Laurent polynomials  $P, Q \in \mathbb{C}[X, 1/X]$  such that  $f^m \circ P = g^n \circ Q$ .
- Solve this for each  $m, n$ , then piece together the solutions.

Summary: From dynamics to number theory to  $F(P) = G(Q)$  to QED.



## Connection with number theory

**Our result:** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)), \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Reformulate: the set of pairs  $(m, n)$  such that  $(f^m(\alpha), g^n(\beta))$  lies on the diagonal  $X = Y$  consists of finitely many “arithmetic progressions” (cosets of cyclic subsemigroups of  $\mathbb{N}^2$ ).

This resembles the **Mordell–Lang** conjecture (proved by **Faltings** and **Vojta**): the intersection of a subvariety  $V$  of a (semi-)abelian variety  $J$  and a finitely-generated subgroup  $G$  of  $J(\mathbb{C})$  consists of finitely many cosets of subgroups of  $G$ .

It also resembles the **Skolem–Mahler–Lech** theorem: if  $a_1, a_2, \dots$  is a sequence of complex numbers satisfying a linear recurrence relation, then the  $n$ 's for which  $a_n = 0$  comprise finitely many arithmetic progressions.

## Connection with number theory

**Our result:** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)), \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Reformulate: the set of pairs  $(m, n)$  such that  $(f^m(\alpha), g^n(\beta))$  lies on the diagonal  $X = Y$  consists of finitely many “arithmetic progressions” (cosets of cyclic subsemigroups of  $\mathbb{N}^2$ ).

This resembles the **Mordell–Lang** conjecture (proved by **Faltings** and **Vojta**): the intersection of a subvariety  $V$  of a (semi-)abelian variety  $J$  and a finitely-generated subgroup  $G$  of  $J(\mathbb{C})$  consists of finitely many cosets of subgroups of  $G$ .

It also resembles the **Skolem–Mahler–Lech** theorem: if  $a_1, a_2, \dots$  is a sequence of complex numbers satisfying a linear recurrence relation, then the  $n$ 's for which  $a_n = 0$  comprise finitely many arithmetic progressions.

## Connection with number theory

**Our result:** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)), \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Reformulate: the set of pairs  $(m, n)$  such that  $(f^m(\alpha), g^n(\beta))$  lies on the diagonal  $X = Y$  consists of finitely many “arithmetic progressions” (cosets of cyclic subsemigroups of  $\mathbb{N}^2$ ).

This resembles the **Mordell–Lang** conjecture (proved by **Faltings** and **Vojta**): the intersection of a subvariety  $V$  of a (semi-)abelian variety  $J$  and a finitely-generated subgroup  $G$  of  $J(\mathbb{C})$  consists of finitely many cosets of subgroups of  $G$ .

It also resembles the **Skolem–Mahler–Lech** theorem: if  $a_1, a_2, \dots$  is a sequence of complex numbers satisfying a linear recurrence relation, then the  $n$ 's for which  $a_n = 0$  comprise finitely many arithmetic progressions.

## Connection with number theory

**Our result:** For  $\alpha, \beta \in \mathbb{C}$  and nonlinear  $f, g \in \mathbb{C}[X]$ , if the orbits  $\{\alpha, f(\alpha), f(f(\alpha)), \dots\}$  and  $\{\beta, g(\beta), g(g(\beta)), \dots\}$  have infinite intersection, then  $f$  and  $g$  have a common iterate.

Reformulate: the set of pairs  $(m, n)$  such that  $(f^m(\alpha), g^n(\beta))$  lies on the diagonal  $X = Y$  consists of finitely many “arithmetic progressions” (cosets of cyclic subsemigroups of  $\mathbb{N}^2$ ).

This resembles the **Mordell–Lang** conjecture (proved by **Faltings** and **Vojta**): the intersection of a subvariety  $V$  of a (semi-)abelian variety  $J$  and a finitely-generated subgroup  $G$  of  $J(\mathbb{C})$  consists of finitely many cosets of subgroups of  $G$ .

It also resembles the **Skolem–Mahler–Lech** theorem: if  $a_1, a_2, \dots$  is a sequence of complex numbers satisfying a linear recurrence relation, then the  $n$ 's for which  $a_n = 0$  comprise finitely many arithmetic progressions.

## A common framework

**Question:** if  $J$  is a variety with a subvariety  $V$  and a point  $\alpha \in J(\mathbb{C})$ , and  $S$  is a finitely-generated commutative semigroup of endomorphisms of  $J$ , then does the set of  $s \in S$  for which  $s(\alpha) \in V$  consist of finitely many cosets of subsemigroups of  $S$ ?

- Yes if  $J = \mathbb{A}^2$  and  $V$  is a line and  $S$  is generated by the maps  $(u, v) \mapsto (f(u), v)$  and  $(u, v) \mapsto (u, g(v))$  for some nonlinear  $f, g \in \mathbb{C}[X]$  (Ghioca, Tucker, Z)
- Yes if  $J$  is a (semi-)abelian variety and  $S$  consists of translations (Faltings, Vojta)
- Yes if  $J = \mathbb{C}^* \times \mathbb{C}$  (Skolem–Mahler–Lech)
- Yes in several other situations (Benedetto, Ghioca, Kurlberg, Scanlon, Tucker, Vojta, Zannier, Z)
- No sometimes.

Note that the proofs in the various cases seem completely unrelated, so a common proof would shed much light.

## A common framework

**Question:** if  $J$  is a variety with a subvariety  $V$  and a point  $\alpha \in J(\mathbb{C})$ , and  $S$  is a finitely-generated commutative semigroup of endomorphisms of  $J$ , then does the set of  $s \in S$  for which  $s(\alpha) \in V$  consist of finitely many cosets of subsemigroups of  $S$ ?

- **Yes** if  $J = \mathbb{A}^2$  and  $V$  is a line and  $S$  is generated by the maps  $(u, v) \mapsto (f(u), v)$  and  $(u, v) \mapsto (u, g(v))$  for some nonlinear  $f, g \in \mathbb{C}[X]$  (Ghioca, Tucker, Z)
- **Yes** if  $J$  is a (semi-)abelian variety and  $S$  consists of translations (Faltings, Vojta)
- **Yes** if  $J = \mathbb{C}^* \times \mathbb{C}$  (Skolem–Mahler–Lech)
- **Yes** in several other situations (Benedetto, Ghioca, Kurlberg, Scanlon, Tucker, Vojta, Zannier, Z)
- **No** sometimes.

Note that the proofs in the various cases seem completely unrelated, so a common proof would shed much light.

## A common framework

**Question:** if  $J$  is a variety with a subvariety  $V$  and a point  $\alpha \in J(\mathbb{C})$ , and  $S$  is a finitely-generated commutative semigroup of endomorphisms of  $J$ , then does the set of  $s \in S$  for which  $s(\alpha) \in V$  consist of finitely many cosets of subsemigroups of  $S$ ?

- **Yes** if  $J = \mathbb{A}^2$  and  $V$  is a line and  $S$  is generated by the maps  $(u, v) \mapsto (f(u), v)$  and  $(u, v) \mapsto (u, g(v))$  for some nonlinear  $f, g \in \mathbb{C}[X]$  (Ghioca, Tucker, Z)
- **Yes** if  $J$  is a (semi-)abelian variety and  $S$  consists of translations (Faltings, Vojta)
- **Yes** if  $J = \mathbb{C}^* \times \mathbb{C}$  (Skolem–Mahler–Lech)
- **Yes** in several other situations (Benedetto, Ghioca, Kurlberg, Scanlon, Tucker, Vojta, Zannier, Z)
- **No** sometimes.

Note that the proofs in the various cases seem completely unrelated, so a common proof would shed much light.

## A common framework

**Question:** if  $J$  is a variety with a subvariety  $V$  and a point  $\alpha \in J(\mathbb{C})$ , and  $S$  is a finitely-generated commutative semigroup of endomorphisms of  $J$ , then does the set of  $s \in S$  for which  $s(\alpha) \in V$  consist of finitely many cosets of subsemigroups of  $S$ ?

- **Yes** if  $J = \mathbb{A}^2$  and  $V$  is a line and  $S$  is generated by the maps  $(u, v) \mapsto (f(u), v)$  and  $(u, v) \mapsto (u, g(v))$  for some nonlinear  $f, g \in \mathbb{C}[X]$  (Ghioca, Tucker, Z)
- **Yes** if  $J$  is a (semi-)abelian variety and  $S$  consists of translations (Faltings, Vojta)
- **Yes** if  $J = \mathbb{C}^* \times \mathbb{C}$  (Skolem–Mahler–Lech)
- **Yes** in several other situations (Benedetto, Ghioca, Kurlberg, Scanlon, Tucker, Vojta, Zannier, Z)
- **No** sometimes.

Note that the proofs in the various cases seem completely unrelated, so a common proof would shed much light.



## A common framework

**Question:** if  $J$  is a variety with a subvariety  $V$  and a point  $\alpha \in J(\mathbb{C})$ , and  $S$  is a finitely-generated commutative semigroup of endomorphisms of  $J$ , then does the set of  $s \in S$  for which  $s(\alpha) \in V$  consist of finitely many cosets of subsemigroups of  $S$ ?

- **Yes** if  $J = \mathbb{A}^2$  and  $V$  is a line and  $S$  is generated by the maps  $(u, v) \mapsto (f(u), v)$  and  $(u, v) \mapsto (u, g(v))$  for some nonlinear  $f, g \in \mathbb{C}[X]$  (Ghioca, Tucker, Z)
- **Yes** if  $J$  is a (semi-)abelian variety and  $S$  consists of translations (Faltings, Vojta)
- **Yes** if  $J = \mathbb{C}^* \times \mathbb{C}$  (Skolem–Mahler–Lech)
- **Yes** in several other situations (Benedetto, Ghioca, Kurlberg, Scanlon, Tucker, Vojta, Zannier, Z)
- **No** sometimes.

Note that the proofs in the various cases seem completely unrelated, so a common proof would shed much light.

## A common framework

**Question:** if  $J$  is a variety with a subvariety  $V$  and a point  $\alpha \in J(\mathbb{C})$ , and  $S$  is a finitely-generated commutative semigroup of endomorphisms of  $J$ , then does the set of  $s \in S$  for which  $s(\alpha) \in V$  consist of finitely many cosets of subsemigroups of  $S$ ?

- **Yes** if  $J = \mathbb{A}^2$  and  $V$  is a line and  $S$  is generated by the maps  $(u, v) \mapsto (f(u), v)$  and  $(u, v) \mapsto (u, g(v))$  for some nonlinear  $f, g \in \mathbb{C}[X]$  (Ghioca, Tucker, Z)
- **Yes** if  $J$  is a (semi-)abelian variety and  $S$  consists of translations (Faltings, Vojta)
- **Yes** if  $J = \mathbb{C}^* \times \mathbb{C}$  (Skolem–Mahler–Lech)
- **Yes** in several other situations (Benedetto, Ghioca, Kurlberg, Scanlon, Tucker, Vojta, Zannier, Z)
- **No** sometimes.

Note that the proofs in the various cases seem completely unrelated, so a common proof would shed much light.

## A common framework

**Question:** if  $J$  is a variety with a subvariety  $V$  and a point  $\alpha \in J(\mathbb{C})$ , and  $S$  is a finitely-generated commutative semigroup of endomorphisms of  $J$ , then does the set of  $s \in S$  for which  $s(\alpha) \in V$  consist of finitely many cosets of subsemigroups of  $S$ ?

- **Yes** if  $J = \mathbb{A}^2$  and  $V$  is a line and  $S$  is generated by the maps  $(u, v) \mapsto (f(u), v)$  and  $(u, v) \mapsto (u, g(v))$  for some nonlinear  $f, g \in \mathbb{C}[X]$  (Ghioca, Tucker, Z)
- **Yes** if  $J$  is a (semi-)abelian variety and  $S$  consists of translations (Faltings, Vojta)
- **Yes** if  $J = \mathbb{C}^* \times \mathbb{C}$  (Skolem–Mahler–Lech)
- **Yes** in several other situations (Benedetto, Ghioca, Kurlberg, Scanlon, Tucker, Vojta, Zannier, Z)
- **No** sometimes.

Note that the proofs in the various cases seem completely unrelated, so a common proof would shed much light.

## Polynomials over the rational numbers

Theorem (Carney–Hortsch–Z)

*For any  $f \in \mathbb{Q}[X]$ , the function  $\mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $c \mapsto f(c)$  is at most 6-to-1 outside a finite set.*

# Polynomials over the rational numbers

Theorem (Carney–Hortsch–Z)

*For any  $f \in \mathbb{Q}[X]$ , the function  $\mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $c \mapsto f(c)$  is at most 6-to-1 outside a finite set.*



# Polynomials over the rational numbers

## Theorem (Carney–Hortsch–Z)

For any  $f \in \mathbb{Q}[X]$ , the function  $\mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $c \mapsto f(c)$  is at most 6-to-1 outside a finite set.

This result is best possible:

- The “finite set” cannot be avoided: there are polynomials inducing any prescribed function on any finite set (**Lagrange**).
- The “6” cannot be improved: for  $f(X) := (X^3 - X)^2$ ,

$$f\left(\pm \frac{2t-1}{t^2-t+1}\right) = f\left(\pm \frac{t^2-1}{t^2-t+1}\right) = f\left(\pm \frac{t^2-2t}{t^2-t+1}\right)$$

for each  $t \in \mathbb{Q}$ .

# Polynomials over the rational numbers

## Theorem (Carney–Hortsch–Z)

For any  $f \in \mathbb{Q}[X]$ , the function  $\mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $c \mapsto f(c)$  is at most 6-to-1 outside a finite set.

This result is best possible:

- The “finite set” cannot be avoided: there are polynomials inducing any prescribed function on any finite set (**Lagrange**).
- The “6” cannot be improved: for  $f(X) := (X^3 - X)^2$ ,

$$f\left(\pm \frac{2t-1}{t^2-t+1}\right) = f\left(\pm \frac{t^2-1}{t^2-t+1}\right) = f\left(\pm \frac{t^2-2t}{t^2-t+1}\right)$$

for each  $t \in \mathbb{Q}$ .

## $f(P) = g(Q)$ and polynomials over the rational numbers

**Theorem (Carney–Hortsch–Z)** For any  $f \in \mathbb{Q}[X]$ , the function  $\mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $c \mapsto f(c)$  is at most 6-to-1 outside a finite set.

Proof sketch:

- If  $f$  is  $(\geq 7)$ -to-1 infinitely often, then there are infinitely many rational points on some subvariety of  $f(X_1) = f(X_2) = \dots = f(X_7)$  which is not contained in any diagonal  $X_i = X_j$  (with  $i \neq j$ ).
- This subvariety is a curve, and by Faltings' theorem (1983) its genus is 0 or 1.
- Equivalently,  $f \circ P_1 = f \circ P_2 = \dots = f \circ P_7$  where the  $P_i$  are distinct (rational or elliptic) functions.
- Solve  $f \circ P = f \circ Q$ , then deduce full results via Ritt's results (again!), determinations of Galois groups of (infinitely many) polynomials, computations of ranks of elliptic curves, Swan conductors, etc.



# $f(P) = g(Q)$ and polynomials over the rational numbers

**Theorem (Carney–Hortsch–Z)** For any  $f \in \mathbb{Q}[X]$ , the function  $\mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $c \mapsto f(c)$  is at most 6-to-1 outside a finite set.

Proof sketch:

- If  $f$  is  $(\geq 7)$ -to-1 infinitely often, then there are infinitely many rational points on some subvariety of  $f(X_1) = f(X_2) = \dots = f(X_7)$  which is not contained in any diagonal  $X_i = X_j$  (with  $i \neq j$ ).
- This subvariety is a curve, and by Faltings' theorem (1983) its genus is 0 or 1.
- Equivalently,  $f \circ P_1 = f \circ P_2 = \dots = f \circ P_7$  where the  $P_i$  are distinct (rational or elliptic) functions.
- Solve  $f \circ P = f \circ Q$ , then deduce full results via Ritt's results (again!), determinations of Galois groups of (infinitely many) polynomials, computations of ranks of elliptic curves, Swan conductors, etc.

# $f(P) = g(Q)$ and polynomials over the rational numbers

**Theorem (Carney–Hortsch–Z)** For any  $f \in \mathbb{Q}[X]$ , the function  $\mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $c \mapsto f(c)$  is at most 6-to-1 outside a finite set.

Proof sketch:

- If  $f$  is  $(\geq 7)$ -to-1 infinitely often, then there are infinitely many rational points on some subvariety of  $f(X_1) = f(X_2) = \dots = f(X_7)$  which is not contained in any diagonal  $X_i = X_j$  (with  $i \neq j$ ).
- This subvariety is a curve, and by Faltings' theorem (1983) its genus is 0 or 1.
- Equivalently,  $f \circ P_1 = f \circ P_2 = \dots = f \circ P_7$  where the  $P_i$  are distinct (rational or elliptic) functions.
- Solve  $f \circ P = f \circ Q$ , then deduce full results via Ritt's results (again!), determinations of Galois groups of (infinitely many) polynomials, computations of ranks of elliptic curves, Swan conductors, etc.

## $f(P) = g(Q)$ and polynomials over the rational numbers

**Theorem (Carney–Hortsch–Z)** For any  $f \in \mathbb{Q}[X]$ , the function  $\mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $c \mapsto f(c)$  is at most 6-to-1 outside a finite set.

Proof sketch:

- If  $f$  is  $(\geq 7)$ -to-1 infinitely often, then there are infinitely many rational points on some subvariety of  $f(X_1) = f(X_2) = \dots = f(X_7)$  which is not contained in any diagonal  $X_i = X_j$  (with  $i \neq j$ ).
- This subvariety is a curve, and by Faltings' theorem (1983) its genus is 0 or 1.
- Equivalently,  $f \circ P_1 = f \circ P_2 = \dots = f \circ P_7$  where the  $P_i$  are distinct (rational or elliptic) functions.
- Solve  $f \circ P = f \circ Q$ , then deduce full results via Ritt's results (again!), determinations of Galois groups of (infinitely many) polynomials, computations of ranks of elliptic curves, Swan conductors, etc.

## $f(P) = g(Q)$ and polynomials over the rational numbers

**Theorem (Carney–Hortsch–Z)** For any  $f \in \mathbb{Q}[X]$ , the function  $\mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $c \mapsto f(c)$  is at most 6-to-1 outside a finite set.

Proof sketch:

- If  $f$  is  $(\geq 7)$ -to-1 infinitely often, then there are infinitely many rational points on some subvariety of  $f(X_1) = f(X_2) = \dots = f(X_7)$  which is not contained in any diagonal  $X_i = X_j$  (with  $i \neq j$ ).
- This subvariety is a curve, and by Faltings' theorem (1983) its genus is 0 or 1.
- Equivalently,  $f \circ P_1 = f \circ P_2 = \dots = f \circ P_7$  where the  $P_i$  are distinct (rational or elliptic) functions.
- Solve  $f \circ P = f \circ Q$ , then deduce full results via Ritt's results (again!), determinations of Galois groups of (infinitely many) polynomials, computations of ranks of elliptic curves, Swan conductors, etc.

## $f(P) = g(Q)$ and polynomials over the rational numbers

**Theorem (Carney–Hortsch–Z)** For any  $f \in \mathbb{Q}[X]$ , the function  $\mathbb{Q} \rightarrow \mathbb{Q}$  defined by  $c \mapsto f(c)$  is at most 6-to-1 outside a finite set.

Proof sketch:

- If  $f$  is  $(\geq 7)$ -to-1 infinitely often, then there are infinitely many rational points on some subvariety of  $f(X_1) = f(X_2) = \dots = f(X_7)$  which is not contained in any diagonal  $X_i = X_j$  (with  $i \neq j$ ).
- This subvariety is a curve, and by Faltings' theorem (1983) its genus is 0 or 1.
- Equivalently,  $f \circ P_1 = f \circ P_2 = \dots = f \circ P_7$  where the  $P_i$  are distinct (rational or elliptic) functions.
- Solve  $f \circ P = f \circ Q$ , then deduce full results via Ritt's results (again!), determinations of Galois groups of (infinitely many) polynomials, computations of ranks of elliptic curves, Swan conductors, etc.

## A plausible generalization

**Theorem (Mazur, 1977):** Any elliptic curve  $Y^2 = X^3 + aX + b$  over  $\mathbb{Q}$  has at most 16 rational torsion points.

**Reformulation:** For any nonconstant morphism  $f: E_1 \rightarrow E_2$  between genus-1 curves over  $\mathbb{Q}$ , the induced map  $f: E_1(\mathbb{Q}) \rightarrow E_2(\mathbb{Q})$  is at most 16-to-1.

**Our result:** For any morphism  $f: \mathbb{A}^1 \rightarrow \mathbb{A}^1$  over  $\mathbb{Q}$ , the induced map  $\mathbb{A}^1(\mathbb{Q}) \rightarrow \mathbb{A}^1(\mathbb{Q})$  is at most 6-to-1 outside a finite set.

**Speculation:** Perhaps, for any morphism  $f: V_1 \rightarrow V_2$  between  $d$ -dimensional varieties over  $\mathbb{Q}$ , the map  $f: V_1(\mathbb{Q}) \rightarrow V_2(\mathbb{Q})$  is at most  $c(d)$ -to-1 outside a lower-dimensional locus ("proper Zariski-closed subset of  $V_2$ ").

## A plausible generalization

**Theorem (Mazur, 1977):** Any elliptic curve  $Y^2 = X^3 + aX + b$  over  $\mathbb{Q}$  has at most 16 rational torsion points.

**Reformulation:** For any nonconstant morphism  $f: E_1 \rightarrow E_2$  between genus-1 curves over  $\mathbb{Q}$ , the induced map  $f: E_1(\mathbb{Q}) \rightarrow E_2(\mathbb{Q})$  is at most 16-to-1.

**Our result:** For any morphism  $f: \mathbb{A}^1 \rightarrow \mathbb{A}^1$  over  $\mathbb{Q}$ , the induced map  $\mathbb{A}^1(\mathbb{Q}) \rightarrow \mathbb{A}^1(\mathbb{Q})$  is at most 6-to-1 outside a finite set.

**Speculation:** Perhaps, for any morphism  $f: V_1 \rightarrow V_2$  between  $d$ -dimensional varieties over  $\mathbb{Q}$ , the map  $f: V_1(\mathbb{Q}) \rightarrow V_2(\mathbb{Q})$  is at most  $c(d)$ -to-1 outside a lower-dimensional locus ("proper Zariski-closed subset of  $V_2$ ").

## A plausible generalization

**Theorem (Mazur, 1977):** Any elliptic curve  $Y^2 = X^3 + aX + b$  over  $\mathbb{Q}$  has at most 16 rational torsion points.

**Reformulation:** For any nonconstant morphism  $f: E_1 \rightarrow E_2$  between genus-1 curves over  $\mathbb{Q}$ , the induced map  $f: E_1(\mathbb{Q}) \rightarrow E_2(\mathbb{Q})$  is at most 16-to-1.

**Our result:** For any morphism  $f: \mathbb{A}^1 \rightarrow \mathbb{A}^1$  over  $\mathbb{Q}$ , the induced map  $\mathbb{A}^1(\mathbb{Q}) \rightarrow \mathbb{A}^1(\mathbb{Q})$  is at most 6-to-1 *outside a finite set*.

**Speculation:** Perhaps, for any morphism  $f: V_1 \rightarrow V_2$  between  $d$ -dimensional varieties over  $\mathbb{Q}$ , the map  $f: V_1(\mathbb{Q}) \rightarrow V_2(\mathbb{Q})$  is at most  $c(d)$ -to-1 outside a lower-dimensional locus ("proper Zariski-closed subset of  $V_2$ ").



## A plausible generalization

**Theorem (Mazur, 1977):** Any elliptic curve  $Y^2 = X^3 + aX + b$  over  $\mathbb{Q}$  has at most 16 rational torsion points.

**Reformulation:** For any nonconstant morphism  $f: E_1 \rightarrow E_2$  between genus-1 curves over  $\mathbb{Q}$ , the induced map  $f: E_1(\mathbb{Q}) \rightarrow E_2(\mathbb{Q})$  is at most 16-to-1.

**Our result:** For any morphism  $f: \mathbb{A}^1 \rightarrow \mathbb{A}^1$  over  $\mathbb{Q}$ , the induced map  $\mathbb{A}^1(\mathbb{Q}) \rightarrow \mathbb{A}^1(\mathbb{Q})$  is at most 6-to-1 *outside a finite set*.

**Speculation:** Perhaps, for any morphism  $f: V_1 \rightarrow V_2$  between  $d$ -dimensional varieties over  $\mathbb{Q}$ , the map  $f: V_1(\mathbb{Q}) \rightarrow V_2(\mathbb{Q})$  is at most  $c(d)$ -to-1 outside a lower-dimensional locus (“proper Zariski-closed subset of  $V_2$ ”).

# Square values of polynomials

**Theorem (Mazur, 1977):** *If  $f(X) \in \mathbb{Q}[X]$  has degree 3 and no multiple roots, and  $f$  takes at least eight square values on  $\mathbb{Q}$ , then  $f$  takes infinitely many square values on  $\mathbb{Q}$ .*

**Theorem (Bhargava, 2013):** *For any  $d \geq 3$ , a positive proportion of squarefree degree- $d$  polynomials in  $\mathbb{Q}[X]$  do not take any square values.*

**Theorem (Faltings, 1983):** *Any squarefree  $f(X) \in \mathbb{Q}[X]$  of degree at least 5 takes only finitely many square values.*

**Conjecture (Caporaso–Harris–Mazur, 1997):** *The number of square values in this result can be bounded solely in terms of  $\deg(f)$ . (The current world record for degree 5 polynomials is 321 square values.)*

# Square values of polynomials

**Theorem (Mazur, 1977):** *If  $f(X) \in \mathbb{Q}[X]$  has degree 3 and no multiple roots, and  $f$  takes at least eight square values on  $\mathbb{Q}$ , then  $f$  takes infinitely many square values on  $\mathbb{Q}$ .*

**Theorem (Bhargava, 2013):** *For any  $d \geq 3$ , a positive proportion of squarefree degree- $d$  polynomials in  $\mathbb{Q}[X]$  do not take any square values.*

**Theorem (Faltings, 1983):** *Any squarefree  $f(X) \in \mathbb{Q}[X]$  of degree at least 5 takes only finitely many square values.*

**Conjecture (Caporaso–Harris–Mazur, 1997):** *The number of square values in this result can be bounded solely in terms of  $\deg(f)$ . (The current world record for degree 5 polynomials is 321 square values.)*

# Square values of polynomials

**Theorem (Mazur, 1977):** *If  $f(X) \in \mathbb{Q}[X]$  has degree 3 and no multiple roots, and  $f$  takes at least eight square values on  $\mathbb{Q}$ , then  $f$  takes infinitely many square values on  $\mathbb{Q}$ .*

**Theorem (Bhargava, 2013):** *For any  $d \geq 3$ , a positive proportion of squarefree degree- $d$  polynomials in  $\mathbb{Q}[X]$  do not take any square values.*

**Theorem (Faltings, 1983):** *Any squarefree  $f(X) \in \mathbb{Q}[X]$  of degree at least 5 takes only finitely many square values.*

**Conjecture (Caporaso–Harris–Mazur, 1997):** *The number of square values in this result can be bounded solely in terms of  $\deg(f)$ . (The current world record for degree 5 polynomials is 321 square values.)*

# Square values of polynomials

**Theorem (Mazur, 1977):** *If  $f(X) \in \mathbb{Q}[X]$  has degree 3 and no multiple roots, and  $f$  takes at least eight square values on  $\mathbb{Q}$ , then  $f$  takes infinitely many square values on  $\mathbb{Q}$ .*

**Theorem (Bhargava, 2013):** *For any  $d \geq 3$ , a positive proportion of squarefree degree- $d$  polynomials in  $\mathbb{Q}[X]$  do not take any square values.*

**Theorem (Faltings, 1983):** *Any squarefree  $f(X) \in \mathbb{Q}[X]$  of degree at least 5 takes only finitely many square values.*

**Conjecture (Caporaso–Harris–Mazur, 1997):** *The number of square values in this result can be bounded solely in terms of  $\deg(f)$ . (The current world record for degree 5 polynomials is 321 square values.)*

# Square values of polynomials

**Theorem (Mazur, 1977):** *If  $f(X) \in \mathbb{Q}[X]$  has degree 3 and no multiple roots, and  $f$  takes at least eight square values on  $\mathbb{Q}$ , then  $f$  takes infinitely many square values on  $\mathbb{Q}$ .*

**Theorem (Bhargava, 2013):** *For any  $d \geq 3$ , a positive proportion of squarefree degree- $d$  polynomials in  $\mathbb{Q}[X]$  do not take any square values.*

**Theorem (Faltings, 1983):** *Any squarefree  $f(X) \in \mathbb{Q}[X]$  of degree at least 5 takes only finitely many square values.*

**Conjecture (Caporaso–Harris–Mazur, 1997):** *The number of square values in this result can be bounded solely in terms of  $\deg(f)$ . (The current world record for degree 5 polynomials is 321 square values.)*

## Common values of two polynomials

**Theorem (CDHHJSWWXZ):** For  $f(X), g(X) \in \overline{\mathbb{Q}}[X] \setminus \mathbb{Q}$ , the equation  $f(X) = g(Y)$  has infinitely many solutions in a number field  $K$  if and only if...

## Common values of two polynomials

**Theorem (CDHHJSWWXZ):** For  $f(X), g(X) \in \overline{\mathbb{Q}}[X] \setminus \mathbb{Q}$ , the equation  $f(X) = g(Y)$  has infinitely many solutions in a number field  $K$  if and only if...





## Common values of two polynomials

**Theorem (CDHHJSWWXZ):** For  $f(X), g(X) \in \overline{\mathbb{Q}}[X] \setminus \mathbb{Q}$ , the equation  $f(X) = g(Y)$  has infinitely many solutions in a number field  $K$  if and only if  $f = L \circ F \circ \ell_1$  and  $g = L \circ G \circ \ell_2$  for some  $L, F, G, \ell_1, \ell_2 \in \overline{\mathbb{Q}}[X]$  such that  $\ell_i$  is linear and (perhaps after switching  $F$  and  $G$ ) either

- $F = X^n$  and  $G$  is either  $X^i H(X)^n$  or  $X^i (X+1)^{n-i} H(X)^n$  or ...
- $F = T_n(X)$  and  $G(X)^2 - 4 = D(X)H(X)^2$  with  $D$  squarefree of degree  $\leq 6$
- $F = X^i (X+1)^j$  and  $G = cX^i (X+1)^j$  for some  $c \in \overline{\mathbb{Q}} \setminus \{0, 1\}$
- $\max(\deg(F), \deg(G)) \leq 16$  and  $F, G$  are on an explicit list.

When  $F = T_n$ :

- We can count the number of corresponding  $G \in \overline{\mathbb{Q}}[X]$  with fixed degree and fixed critical values.
- Solutions  $G \in K[X]$  of degree  $N$  are in bijection with triples  $(C, \sigma, P)$  where  $C$  is a curve/ $K$  of genus  $\leq 2$ ,  $\sigma$  is a “hyperelliptic involution” on  $C$ , and  $P \in C(K)$  satisfies  $N([P] - [\sigma(P)]) = 0$  in  $\text{Jac}(C)$ .

## Common values of two polynomials

**Theorem (CDHHJSWWXZ):** For  $f(X), g(X) \in \overline{\mathbb{Q}}[X] \setminus \mathbb{Q}$ , the equation  $f(X) = g(Y)$  has infinitely many solutions in a number field  $K$  if and only if  $f = L \circ F \circ \ell_1$  and  $g = L \circ G \circ \ell_2$  for some  $L, F, G, \ell_1, \ell_2 \in \overline{\mathbb{Q}}[X]$  such that  $\ell_i$  is linear and (perhaps after switching  $F$  and  $G$ ) either

- $F = X^n$  and  $G$  is either  $X^i H(X)^n$  or  $X^i (X+1)^{n-i} H(X)^n$  or ...
- $F = T_n(X)$  and  $G(X)^2 - 4 = D(X)H(X)^2$  with  $D$  squarefree of degree  $\leq 6$
- $F = X^i (X+1)^j$  and  $G = cX^i (X+1)^j$  for some  $c \in \overline{\mathbb{Q}} \setminus \{0, 1\}$
- $\max(\deg(F), \deg(G)) \leq 16$  and  $F, G$  are on an explicit list.

When  $F = T_n$ :

- We can count the number of corresponding  $G \in \overline{\mathbb{Q}}[X]$  with fixed degree and fixed critical values.
- Solutions  $G \in K[X]$  of degree  $N$  are in bijection with triples  $(C, \sigma, P)$  where  $C$  is a curve/ $K$  of genus  $\leq 2$ ,  $\sigma$  is a “hyperelliptic involution” on  $C$ , and  $P \in C(K)$  satisfies  $N([P] - [\sigma(P)]) = 0$  in  $\text{Jac}(C)$ .

## Common values of two polynomials

**Theorem (CDHHJSWWXZ):** For  $f(X), g(X) \in \overline{\mathbb{Q}}[X] \setminus \mathbb{Q}$ , the equation  $f(X) = g(Y)$  has infinitely many solutions in a number field  $K$  if and only if  $f = L \circ F \circ \ell_1$  and  $g = L \circ G \circ \ell_2$  for some  $L, F, G, \ell_1, \ell_2 \in \overline{\mathbb{Q}}[X]$  such that  $\ell_i$  is linear and (perhaps after switching  $F$  and  $G$ ) either

- $F = X^n$  and  $G$  is either  $X^i H(X)^n$  or  $X^i (X + 1)^{n-i} H(X)^n$  or ...
- $F = T_n(X)$  and  $G(X)^2 - 4 = D(X)H(X)^2$  with  $D$  squarefree of degree  $\leq 6$
- $F = X^i (X + 1)^j$  and  $G = cX^i (X + 1)^j$  for some  $c \in \overline{\mathbb{Q}} \setminus \{0, 1\}$
- $\max(\deg(F), \deg(G)) \leq 16$  and  $F, G$  are on an explicit list.

Proof: by Faltings' theorem and Picard's theorem (see the next slide), the hypotheses are equivalent to asserting that  $f \circ P = g \circ Q$  has a solution with  $P, Q$  being nonconstant meromorphic functions on  $\mathbb{C}$ . So "just" find all such solutions (which is very difficult).

# Meromorphic functions

An *entire function* is a function on  $\mathbb{C}$  given by a power series which converges everywhere.

A *meromorphic function* is the ratio of two entire functions.

*Theorem (Picard, 1887)* For any nonconstant  $F(X, Y) \in \mathbb{C}[X, Y]$ , there exist nonconstant meromorphic  $p(t)$  and  $q(t)$  with  $F(p(t), q(t)) = 0$  if and only if some irreducible factor of  $F(X, Y)$  defines a curve of genus 0 or 1.

Recall *Faltings' theorem*: For any nonconstant  $F(X, Y) \in \mathbb{Q}[X, Y]$ , the equation  $F(X, Y) = 0$  has infinitely many solutions in some number field if and only if some irreducible factor of  $F(X, Y)$  defines a curve of genus 0 or 1.

This is one instance of a tremendously fruitful set of analogies between complex function theory and number theory.

# Meromorphic functions

An *entire function* is a function on  $\mathbb{C}$  given by a power series which converges everywhere.

A *meromorphic function* is the ratio of two entire functions.

*Theorem (Picard, 1887)* For any nonconstant  $F(X, Y) \in \mathbb{C}[X, Y]$ , there exist nonconstant meromorphic  $p(t)$  and  $q(t)$  with  $F(p(t), q(t)) = 0$  if and only if some irreducible factor of  $F(X, Y)$  defines a curve of genus 0 or 1.

Recall *Faltings' theorem*: For any nonconstant  $F(X, Y) \in \mathbb{Q}[X, Y]$ , the equation  $F(X, Y) = 0$  has infinitely many solutions in some number field if and only if some irreducible factor of  $F(X, Y)$  defines a curve of genus 0 or 1.

This is one instance of a tremendously fruitful set of analogies between complex function theory and number theory.

# Meromorphic functions

An *entire function* is a function on  $\mathbb{C}$  given by a power series which converges everywhere.

A *meromorphic function* is the ratio of two entire functions.

**Theorem (Picard, 1887)** *For any nonconstant  $F(X, Y) \in \mathbb{C}[X, Y]$ , there exist nonconstant meromorphic  $p(t)$  and  $q(t)$  with  $F(p(t), q(t)) = 0$  if and only if some irreducible factor of  $F(X, Y)$  defines a curve of genus 0 or 1.*

Recall **Faltings' theorem**: *For any nonconstant  $F(X, Y) \in \mathbb{Q}[X, Y]$ , the equation  $F(X, Y) = 0$  has infinitely many solutions in some number field if and only if some irreducible factor of  $F(X, Y)$  defines a curve of genus 0 or 1.*

This is one instance of a tremendously fruitful set of analogies between complex function theory and number theory.

# Meromorphic functions

An *entire function* is a function on  $\mathbb{C}$  given by a power series which converges everywhere.

A *meromorphic function* is the ratio of two entire functions.

**Theorem (Picard, 1887)** *For any nonconstant  $F(X, Y) \in \mathbb{C}[X, Y]$ , there exist nonconstant meromorphic  $p(t)$  and  $q(t)$  with  $F(p(t), q(t)) = 0$  if and only if some irreducible factor of  $F(X, Y)$  defines a curve of genus 0 or 1.*

Recall **Faltings' theorem**: *For any nonconstant  $F(X, Y) \in \mathbb{Q}[X, Y]$ , the equation  $F(X, Y) = 0$  has infinitely many solutions in some number field if and only if some irreducible factor of  $F(X, Y)$  defines a curve of genus 0 or 1.*

This is one instance of a tremendously fruitful set of analogies between complex function theory and number theory.

# Meromorphic functions

An *entire function* is a function on  $\mathbb{C}$  given by a power series which converges everywhere.

A *meromorphic function* is the ratio of two entire functions.

**Theorem (Picard, 1887)** *For any nonconstant  $F(X, Y) \in \mathbb{C}[X, Y]$ , there exist nonconstant meromorphic  $p(t)$  and  $q(t)$  with  $F(p(t), q(t)) = 0$  if and only if some irreducible factor of  $F(X, Y)$  defines a curve of genus 0 or 1.*

Recall **Faltings' theorem**: *For any nonconstant  $F(X, Y) \in \mathbb{Q}[X, Y]$ , the equation  $F(X, Y) = 0$  has infinitely many solutions in some number field if and only if some irreducible factor of  $F(X, Y)$  defines a curve of genus 0 or 1.*

This is one instance of a tremendously fruitful set of analogies between complex function theory and number theory.



## Value sharing

**Theorem (Nevanlinna, 1926):** *If nonconstant meromorphic functions  $P(t)$  and  $Q(t)$  satisfy  $P^{-1}(\alpha_i) = Q^{-1}(\alpha_i)$  for five distinct values  $\alpha_i \in \mathbb{C}$ , then  $P = Q$ .*

**A much-studied question:** What if  $P^{-1}(S_i) = Q^{-1}(T_i)$  for several pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

**Remark:** If  $f \circ P = g \circ Q$  with  $f, g \in \mathbb{C}(X) \setminus \mathbb{C}$ , then  $P^{-1}(f^{-1}(\gamma)) = Q^{-1}(g^{-1}(\gamma))$  for every  $\gamma \in \mathbb{C}$ .

**Question:** Does this account for all pairs  $(P, Q)$  such that  $P^{-1}(S_i) = Q^{-1}(T_i)$  for infinitely many pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

- Yes if  $P, Q \in \mathbb{C}(X)$  (Beals–Wetherell–Z, 2009 +...)
- Yes if the polynomials  $\prod_{s \in S_i} (X - s)$  and  $\prod_{s \in T_i} (X - s)$  have “few” critical points (Weiss–Z)

## Value sharing

**Theorem (Nevanlinna, 1926):** *If nonconstant meromorphic functions  $P(t)$  and  $Q(t)$  satisfy  $P^{-1}(\alpha_i) = Q^{-1}(\alpha_i)$  for five distinct values  $\alpha_i \in \mathbb{C}$ , then  $P = Q$ .*

**A much-studied question:** What if  $P^{-1}(S_i) = Q^{-1}(T_i)$  for several pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

**Remark:** If  $f \circ P = g \circ Q$  with  $f, g \in \mathbb{C}(X) \setminus \mathbb{C}$ , then  $P^{-1}(f^{-1}(\gamma)) = Q^{-1}(g^{-1}(\gamma))$  for every  $\gamma \in \mathbb{C}$ .

**Question:** Does this account for all pairs  $(P, Q)$  such that  $P^{-1}(S_i) = Q^{-1}(T_i)$  for infinitely many pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

- Yes if  $P, Q \in \mathbb{C}(X)$  (Beals–Wetherell–Z, 2009 +...)
- Yes if the polynomials  $\prod_{s \in S_i} (X - s)$  and  $\prod_{s \in T_i} (X - s)$  have “few” critical points (Weiss–Z)

## Value sharing

**Theorem (Nevanlinna, 1926):** *If nonconstant meromorphic functions  $P(t)$  and  $Q(t)$  satisfy  $P^{-1}(\alpha_i) = Q^{-1}(\alpha_i)$  for five distinct values  $\alpha_i \in \mathbb{C}$ , then  $P = Q$ .*

**A much-studied question:** What if  $P^{-1}(S_i) = Q^{-1}(T_i)$  for several pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

**Remark:** If  $f \circ P = g \circ Q$  with  $f, g \in \mathbb{C}(X) \setminus \mathbb{C}$ , then  $P^{-1}(f^{-1}(\gamma)) = Q^{-1}(g^{-1}(\gamma))$  for every  $\gamma \in \mathbb{C}$ .

**Question:** Does this account for all pairs  $(P, Q)$  such that  $P^{-1}(S_i) = Q^{-1}(T_i)$  for infinitely many pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

- Yes if  $P, Q \in \mathbb{C}(X)$  (Beals–Wetherell–Z, 2009 +...)
- Yes if the polynomials  $\prod_{s \in S_i} (X - s)$  and  $\prod_{s \in T_i} (X - s)$  have “few” critical points (Weiss–Z)

## Value sharing

**Theorem (Nevanlinna, 1926):** *If nonconstant meromorphic functions  $P(t)$  and  $Q(t)$  satisfy  $P^{-1}(\alpha_i) = Q^{-1}(\alpha_i)$  for five distinct values  $\alpha_i \in \mathbb{C}$ , then  $P = Q$ .*

**A much-studied question:** What if  $P^{-1}(S_i) = Q^{-1}(T_i)$  for several pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

**Remark:** If  $f \circ P = g \circ Q$  with  $f, g \in \mathbb{C}(X) \setminus \mathbb{C}$ , then  $P^{-1}(f^{-1}(\gamma)) = Q^{-1}(g^{-1}(\gamma))$  for every  $\gamma \in \mathbb{C}$ .

**Question:** Does this account for all pairs  $(P, Q)$  such that  $P^{-1}(S_i) = Q^{-1}(T_i)$  for infinitely many pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

- Yes if  $P, Q \in \mathbb{C}(X)$  (Beals–Wetherell–Z, 2009 +...)
- Yes if the polynomials  $\prod_{s \in S_i} (X - s)$  and  $\prod_{s \in T_i} (X - s)$  have “few” critical points (Weiss–Z)

## Value sharing

**Theorem (Nevanlinna, 1926):** *If nonconstant meromorphic functions  $P(t)$  and  $Q(t)$  satisfy  $P^{-1}(\alpha_i) = Q^{-1}(\alpha_i)$  for five distinct values  $\alpha_i \in \mathbb{C}$ , then  $P = Q$ .*

**A much-studied question:** What if  $P^{-1}(S_i) = Q^{-1}(T_i)$  for several pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

**Remark:** If  $f \circ P = g \circ Q$  with  $f, g \in \mathbb{C}(X) \setminus \mathbb{C}$ , then  $P^{-1}(f^{-1}(\gamma)) = Q^{-1}(g^{-1}(\gamma))$  for every  $\gamma \in \mathbb{C}$ .

**Question:** Does this account for all pairs  $(P, Q)$  such that  $P^{-1}(S_i) = Q^{-1}(T_i)$  for infinitely many pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

- **Yes** if  $P, Q \in \mathbb{C}(X)$  (Beals–Wetherell–Z, 2009 +...)
- **Yes** if the polynomials  $\prod_{s \in S_i} (X - s)$  and  $\prod_{s \in T_i} (X - s)$  have “few” critical points (Weiss–Z)

## Value sharing

**Theorem (Nevanlinna, 1926):** *If nonconstant meromorphic functions  $P(t)$  and  $Q(t)$  satisfy  $P^{-1}(\alpha_i) = Q^{-1}(\alpha_i)$  for five distinct values  $\alpha_i \in \mathbb{C}$ , then  $P = Q$ .*

**A much-studied question:** What if  $P^{-1}(S_i) = Q^{-1}(T_i)$  for several pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

**Remark:** If  $f \circ P = g \circ Q$  with  $f, g \in \mathbb{C}(X) \setminus \mathbb{C}$ , then  $P^{-1}(f^{-1}(\gamma)) = Q^{-1}(g^{-1}(\gamma))$  for every  $\gamma \in \mathbb{C}$ .

**Question:** Does this account for all pairs  $(P, Q)$  such that  $P^{-1}(S_i) = Q^{-1}(T_i)$  for infinitely many pairs  $(S_i, T_i)$  of finite subsets of  $\mathbb{C}$ ?

- **Yes** if  $P, Q \in \mathbb{C}(X)$  (Beals–Wetherell–Z, 2009 +...)
- **Yes** if the polynomials  $\prod_{s \in S_i} (X - s)$  and  $\prod_{s \in T_i} (X - s)$  have “few” critical points (Weiss–Z)

## Value sharing and functional equations

**Sample theorem (Weiss-Z):** *If nonconstant meromorphic functions  $P(t)$  and  $Q(t)$  and nonempty finite  $S, T \subset \mathbb{C}$  satisfy  $P^{-1}(S) = Q^{-1}(T)$ , and at most  $\min(\#S, \#T) - 13$  complex numbers are critical points of  $f(X) := \prod_{s \in S}(X - s)$  and/or  $g(X) := \prod_{s \in T}(X - s)$ , then*

$$f(P(t)) = \frac{g(Q(t))}{c \cdot g(Q(t)) + d} \quad (*)$$

*for some  $c, d \in \mathbb{C}$ .*

**Theorem (CDHHHJSWWXZ):** *We know all  $f, g \in \mathbb{C}[X]$  and meromorphic  $P, Q$  satisfying  $(*)$ .*

## Value sharing and functional equations

**Sample theorem (Weiss–Z):** *If nonconstant meromorphic functions  $P(t)$  and  $Q(t)$  and nonempty finite  $S, T \subset \mathbb{C}$  satisfy  $P^{-1}(S) = Q^{-1}(T)$ , and at most  $\min(\#S, \#T) - 13$  complex numbers are critical points of  $f(X) := \prod_{s \in S}(X - s)$  and/or  $g(X) := \prod_{s \in T}(X - s)$ , then*

$$f(P(t)) = \frac{g(Q(t))}{c \cdot g(Q(t)) + d} \quad (*)$$

for some  $c, d \in \mathbb{C}$ .

**Theorem (CDHHHJSWWXZ):** *We know all  $f, g \in \mathbb{C}[X]$  and meromorphic  $P, Q$  satisfying  $(*)$ .*



## How we solved $f(P) = g(Q)$ in polynomials $f, g$ and meromorphic $P, Q$

By **Picard's theorem** and uniqueness of meromorphic parametrizations, the problem amounts to determining when  $f(X) = g(Y)$  has a component of genus 0 or 1.

First classify  $f, g \in \mathbb{C}[X]$  for which  $f(X) - g(Y)$  is *irreducible* and defines a curve of genus  $\leq 1$ .

The genus  $g$  of  $f(X) = g(Y)$  can be expressed in terms of the factorization types of all  $f(X) - \lambda$  and  $g(X) - \lambda$  in  $\mathbb{C}[X]$  (with  $\lambda \in \mathbb{C}$ ).

Use this to determine all numerical plausibilities for the factorization types of all  $f(X) - \lambda$ , assuming  $f(X) - g(Y)$  irreducible and  $g \in \{0, 1\}$ .

Then determine all corresponding polynomials via computations in fundamental groups, Riemann's existence theorem, and solutions of differential equations.

## How we solved $f(P) = g(Q)$ in polynomials $f, g$ and meromorphic $P, Q$

By **Picard's theorem** and uniqueness of meromorphic parametrizations, the problem amounts to determining when  $f(X) = g(Y)$  has a component of genus 0 or 1.

First classify  $f, g \in \mathbb{C}[X]$  for which  $f(X) - g(Y)$  is *irreducible* and defines a curve of genus  $\leq 1$ .

The genus  $g$  of  $f(X) = g(Y)$  can be expressed in terms of the factorization types of all  $f(X) - \lambda$  and  $g(X) - \lambda$  in  $\mathbb{C}[X]$  (with  $\lambda \in \mathbb{C}$ ).

Use this to determine all numerical plausibilities for the factorization types of all  $f(X) - \lambda$ , assuming  $f(X) - g(Y)$  irreducible and  $g \in \{0, 1\}$ .

Then determine all corresponding polynomials via computations in fundamental groups, Riemann's existence theorem, and solutions of differential equations.

## How we solved $f(P) = g(Q)$ in polynomials $f, g$ and meromorphic $P, Q$

By **Picard's theorem** and uniqueness of meromorphic parametrizations, the problem amounts to determining when  $f(X) = g(Y)$  has a component of genus 0 or 1.

First classify  $f, g \in \mathbb{C}[X]$  for which  $f(X) - g(Y)$  is *irreducible* and defines a curve of genus  $\leq 1$ .

The genus  $g$  of  $f(X) = g(Y)$  can be expressed in terms of the factorization types of all  $f(X) - \lambda$  and  $g(X) - \lambda$  in  $\mathbb{C}[X]$  (with  $\lambda \in \mathbb{C}$ ).

Use this to determine all numerical plausibilities for the factorization types of all  $f(X) - \lambda$ , assuming  $f(X) - g(Y)$  irreducible and  $g \in \{0, 1\}$ .

Then determine all corresponding polynomials via computations in fundamental groups, Riemann's existence theorem, and solutions of differential equations.

## How we solved $f(P) = g(Q)$ in polynomials $f, g$ and meromorphic $P, Q$

By **Picard's theorem** and uniqueness of meromorphic parametrizations, the problem amounts to determining when  $f(X) = g(Y)$  has a component of genus 0 or 1.

First classify  $f, g \in \mathbb{C}[X]$  for which  $f(X) - g(Y)$  is *irreducible* and defines a curve of genus  $\leq 1$ .

The genus  $g$  of  $f(X) = g(Y)$  can be expressed in terms of the factorization types of all  $f(X) - \lambda$  and  $g(X) - \lambda$  in  $\mathbb{C}[X]$  (with  $\lambda \in \mathbb{C}$ ).

Use this to determine all numerical plausibilities for the factorization types of all  $f(X) - \lambda$ , assuming  $f(X) - g(Y)$  irreducible and  $g \in \{0, 1\}$ .

Then determine all corresponding polynomials via computations in fundamental groups, Riemann's existence theorem, and solutions of differential equations.

## How we solved $f(P) = g(Q)$ in polynomials $f, g$ and meromorphic $P, Q$

By **Picard's theorem** and uniqueness of meromorphic parametrizations, the problem amounts to determining when  $f(X) = g(Y)$  has a component of genus 0 or 1.

First classify  $f, g \in \mathbb{C}[X]$  for which  $f(X) - g(Y)$  is *irreducible* and defines a curve of genus  $\leq 1$ .

The genus  $g$  of  $f(X) = g(Y)$  can be expressed in terms of the factorization types of all  $f(X) - \lambda$  and  $g(X) - \lambda$  in  $\mathbb{C}[X]$  (with  $\lambda \in \mathbb{C}$ ).

Use this to determine all numerical plausibilities for the factorization types of all  $f(X) - \lambda$ , assuming  $f(X) - g(Y)$  irreducible and  $g \in \{0, 1\}$ .

Then determine all corresponding polynomials via computations in fundamental groups, Riemann's existence theorem, and solutions of differential equations.

## The reducible case

We cannot immediately resolve the reducible case after solving the irreducible case, since factors of  $f(X) - g(Y)$  generally cannot be written in this form. Instead we pass from the **decomposable** case to the **indecomposable** case, using several ingredients including:

**Theorem** (Hallett–Wells–Xia–Z, building on Fried, 1973; Feit, 1973; Feit, 1980; Müller, 1993; Cassou-Noguès–Couveignes, 1999; Elkies, 2012) *We explicitly know all indecomposable  $f(X) \in \mathbb{C}[X]$  for which the Galois group of  $f(X) - t$  over  $\mathbb{C}(t)$  is neither  $S_n$  nor  $A_n$  (where  $n := \deg(f)$ ).*

Note: the proof of this Theorem crucially uses consequences of the classification of finite simple groups.

**Corollary:** *If  $f, g \in \mathbb{C}[X]$  are indecomposable and  $f(X) - g(Y)$  is reducible then either  $g = f \circ h$  (with  $h$  linear) or  $\deg(f) = \deg(g) \leq 31$  and  $f, g$  are explicitly known.*

## The reducible case

We cannot immediately resolve the reducible case after solving the irreducible case, since factors of  $f(X) - g(Y)$  generally cannot be written in this form. Instead we pass from the **decomposable** case to the **indecomposable** case, using several ingredients including:

**Theorem** (Hallett–Wells–Xia–Z, building on Fried, 1973; Feit, 1973; Feit, 1980; Müller, 1993; Cassou-Noguès–Couveignes, 1999; Elkies, 2012) *We explicitly know all indecomposable  $f(X) \in \mathbb{C}[X]$  for which the Galois group of  $f(X) - t$  over  $\mathbb{C}(t)$  is neither  $S_n$  nor  $A_n$  (where  $n := \deg(f)$ ).*

Note: the proof of this Theorem crucially uses consequences of the classification of finite simple groups.

**Corollary:** *If  $f, g \in \mathbb{C}[X]$  are indecomposable and  $f(X) - g(Y)$  is reducible then either  $g = f \circ h$  (with  $h$  linear) or  $\deg(f) = \deg(g) \leq 31$  and  $f, g$  are explicitly known.*

## The reducible case

We cannot immediately resolve the reducible case after solving the irreducible case, since factors of  $f(X) - g(Y)$  generally cannot be written in this form. Instead we pass from the **decomposable** case to the **indecomposable** case, using several ingredients including:

**Theorem** (Hallett–Wells–Xia–Z, building on Fried, 1973; Feit, 1973; Feit, 1980; Müller, 1993; Cassou-Noguès–Couveignes, 1999; Elkies, 2012) *We explicitly know all indecomposable  $f(X) \in \mathbb{C}[X]$  for which the Galois group of  $f(X) - t$  over  $\mathbb{C}(t)$  is neither  $S_n$  nor  $A_n$  (where  $n := \deg(f)$ ).*

Note: the proof of this Theorem crucially uses consequences of the classification of finite simple groups.

**Corollary:** *If  $f, g \in \mathbb{C}[X]$  are indecomposable and  $f(X) - g(Y)$  is reducible then either  $g = f \circ h$  (with  $h$  linear) or  $\deg(f) = \deg(g) \leq 31$  and  $f, g$  are explicitly known.*



## The reducible case

We cannot immediately resolve the reducible case after solving the irreducible case, since factors of  $f(X) - g(Y)$  generally cannot be written in this form. Instead we pass from the **decomposable** case to the **indecomposable** case, using several ingredients including:

**Theorem** (Hallett–Wells–Xia–Z, building on Fried, 1973; Feit, 1973; Feit, 1980; Müller, 1993; Cassou-Noguès–Couveignes, 1999; Elkies, 2012) *We explicitly know all indecomposable  $f(X) \in \mathbb{C}[X]$  for which the Galois group of  $f(X) - t$  over  $\mathbb{C}(t)$  is neither  $S_n$  nor  $A_n$  (where  $n := \deg(f)$ ).*

Note: the proof of this Theorem crucially uses consequences of the classification of finite simple groups.

*Corollary: If  $f, g \in \mathbb{C}[X]$  are indecomposable and  $f(X) - g(Y)$  is reducible then either  $g = f \circ h$  (with  $h$  linear) or  $\deg(f) = \deg(g) \leq 31$  and  $f, g$  are explicitly known.*

## The reducible case

We cannot immediately resolve the reducible case after solving the irreducible case, since factors of  $f(X) - g(Y)$  generally cannot be written in this form. Instead we pass from the **decomposable** case to the **indecomposable** case, using several ingredients including:

**Theorem** (Hallett–Wells–Xia–Z, building on Fried, 1973; Feit, 1973; Feit, 1980; Müller, 1993; Cassou-Noguès–Couveignes, 1999; Elkies, 2012) *We explicitly know all indecomposable  $f(X) \in \mathbb{C}[X]$  for which the Galois group of  $f(X) - t$  over  $\mathbb{C}(t)$  is neither  $S_n$  nor  $A_n$  (where  $n := \deg(f)$ ).*

Note: the proof of this Theorem crucially uses consequences of the classification of finite simple groups.

**Corollary:** *If  $f, g \in \mathbb{C}[X]$  are indecomposable and  $f(X) - g(Y)$  is reducible then either  $g = f \circ h$  (with  $h$  linear) or  $\deg(f) = \deg(g) \leq 31$  and  $f, g$  are explicitly known.*

## Summary

Solutions of instances of  $f \circ P = g \circ Q$  in polynomials  $f, g$  and meromorphic  $P, Q$  have been applied to:

- Describing intersections of orbits of complex polynomials
- Showing that for  $f \in \mathbb{Q}[X]$  the function  $f: \mathbb{Q} \rightarrow \mathbb{Q}$  is at most 6-to-1 outside a finite set
- Finding all  $f, g \in \overline{\mathbb{Q}}[X]$  such that  $f(K) \cap g(K)$  is infinite for some number field  $K$
- Determining nonempty finite  $S, T \subset \mathbb{C}$  such that  $P^{-1}(S) \neq Q^{-1}(T)$  for any nonconstant meromorphic  $P, Q$
- Solving  $f^{-1}(U) = g^{-1}(V)$  in  $f, g \in \mathbb{C}[X]$  and infinite compact  $U, V \subset \mathbb{C}$  (Dinh 2005; Pakovich 2008)
- Determining all subvarieties of  $\mathbb{A}^n$  having an endomorphism of the form  $(x_1, \dots, x_n) \mapsto (f_1(x_1), \dots, f_n(x_n))$  where each  $f_i \in \mathbb{C}[X]$  has degree  $\geq 2$  (Medvedev–Scanlon, 2013)
- and several other topics.

## Summary

Solutions of instances of  $f \circ P = g \circ Q$  in polynomials  $f, g$  and meromorphic  $P, Q$  have been applied to:

- Describing intersections of orbits of complex polynomials
- Showing that for  $f \in \mathbb{Q}[X]$  the function  $f: \mathbb{Q} \rightarrow \mathbb{Q}$  is at most 6-to-1 outside a finite set
- Finding all  $f, g \in \overline{\mathbb{Q}}[X]$  such that  $f(K) \cap g(K)$  is infinite for some number field  $K$
- Determining nonempty finite  $S, T \subset \mathbb{C}$  such that  $P^{-1}(S) \neq Q^{-1}(T)$  for any nonconstant meromorphic  $P, Q$
- Solving  $f^{-1}(U) = g^{-1}(V)$  in  $f, g \in \mathbb{C}[X]$  and infinite compact  $U, V \subset \mathbb{C}$  (Dinh 2005; Pakovich 2008)
- Determining all subvarieties of  $\mathbb{A}^n$  having an endomorphism of the form  $(x_1, \dots, x_n) \mapsto (f_1(x_1), \dots, f_n(x_n))$  where each  $f_i \in \mathbb{C}[X]$  has degree  $\geq 2$  (Medvedev–Scanlon, 2013)
- and several other topics.

## Summary

Solutions of instances of  $f \circ P = g \circ Q$  in polynomials  $f, g$  and meromorphic  $P, Q$  have been applied to:

- Describing intersections of orbits of complex polynomials
- Showing that for  $f \in \mathbb{Q}[X]$  the function  $f: \mathbb{Q} \rightarrow \mathbb{Q}$  is at most 6-to-1 outside a finite set
- Finding all  $f, g \in \overline{\mathbb{Q}}[X]$  such that  $f(K) \cap g(K)$  is infinite for some number field  $K$
- Determining nonempty finite  $S, T \subset \mathbb{C}$  such that  $P^{-1}(S) \neq Q^{-1}(T)$  for any nonconstant meromorphic  $P, Q$
- Solving  $f^{-1}(U) = g^{-1}(V)$  in  $f, g \in \mathbb{C}[X]$  and infinite compact  $U, V \subset \mathbb{C}$  (Dinh 2005; Pakovich 2008)
- Determining all subvarieties of  $\mathbb{A}^n$  having an endomorphism of the form  $(x_1, \dots, x_n) \mapsto (f_1(x_1), \dots, f_n(x_n))$  where each  $f_i \in \mathbb{C}[X]$  has degree  $\geq 2$  (Medvedev–Scanlon, 2013)
- and several other topics.

## Summary

Solutions of instances of  $f \circ P = g \circ Q$  in polynomials  $f, g$  and meromorphic  $P, Q$  have been applied to:

- Describing intersections of orbits of complex polynomials
- Showing that for  $f \in \mathbb{Q}[X]$  the function  $f: \mathbb{Q} \rightarrow \mathbb{Q}$  is at most 6-to-1 outside a finite set
- Finding all  $f, g \in \overline{\mathbb{Q}}[X]$  such that  $f(K) \cap g(K)$  is infinite for some number field  $K$
- Determining nonempty finite  $S, T \subset \mathbb{C}$  such that  $P^{-1}(S) \neq Q^{-1}(T)$  for any nonconstant meromorphic  $P, Q$
- Solving  $f^{-1}(U) = g^{-1}(V)$  in  $f, g \in \mathbb{C}[X]$  and infinite compact  $U, V \subset \mathbb{C}$  (Dinh 2005; Pakovich 2008)
- Determining all subvarieties of  $\mathbb{A}^n$  having an endomorphism of the form  $(x_1, \dots, x_n) \mapsto (f_1(x_1), \dots, f_n(x_n))$  where each  $f_i \in \mathbb{C}[X]$  has degree  $\geq 2$  (Medvedev–Scanlon, 2013)
- and several other topics.

## Summary

Solutions of instances of  $f \circ P = g \circ Q$  in polynomials  $f, g$  and meromorphic  $P, Q$  have been applied to:

- Describing intersections of orbits of complex polynomials
- Showing that for  $f \in \mathbb{Q}[X]$  the function  $f: \mathbb{Q} \rightarrow \mathbb{Q}$  is at most 6-to-1 outside a finite set
- Finding all  $f, g \in \overline{\mathbb{Q}}[X]$  such that  $f(K) \cap g(K)$  is infinite for some number field  $K$
- Determining nonempty finite  $S, T \subset \mathbb{C}$  such that  $P^{-1}(S) \neq Q^{-1}(T)$  for any nonconstant meromorphic  $P, Q$
- Solving  $f^{-1}(U) = g^{-1}(V)$  in  $f, g \in \mathbb{C}[X]$  and infinite compact  $U, V \subset \mathbb{C}$  (Dinh 2005; Pakovich 2008)
- Determining all subvarieties of  $\mathbb{A}^n$  having an endomorphism of the form  $(x_1, \dots, x_n) \mapsto (f_1(x_1), \dots, f_n(x_n))$  where each  $f_i \in \mathbb{C}[X]$  has degree  $\geq 2$  (Medvedev–Scanlon, 2013)
- and several other topics.

## Summary

Solutions of instances of  $f \circ P = g \circ Q$  in polynomials  $f, g$  and meromorphic  $P, Q$  have been applied to:

- Describing intersections of orbits of complex polynomials
- Showing that for  $f \in \mathbb{Q}[X]$  the function  $f: \mathbb{Q} \rightarrow \mathbb{Q}$  is at most 6-to-1 outside a finite set
- Finding all  $f, g \in \overline{\mathbb{Q}}[X]$  such that  $f(K) \cap g(K)$  is infinite for some number field  $K$
- Determining nonempty finite  $S, T \subset \mathbb{C}$  such that  $P^{-1}(S) \neq Q^{-1}(T)$  for any nonconstant meromorphic  $P, Q$
- Solving  $f^{-1}(U) = g^{-1}(V)$  in  $f, g \in \mathbb{C}[X]$  and infinite compact  $U, V \subset \mathbb{C}$  (Dinh 2005; Pakovich 2008)
- Determining all subvarieties of  $\mathbb{A}^n$  having an endomorphism of the form  $(x_1, \dots, x_n) \mapsto (f_1(x_1), \dots, f_n(x_n))$  where each  $f_i \in \mathbb{C}[X]$  has degree  $\geq 2$  (Medvedev–Scanlon, 2013)
- and several other topics.



## Summary

Solutions of instances of  $f \circ P = g \circ Q$  in polynomials  $f, g$  and meromorphic  $P, Q$  have been applied to:

- Describing intersections of orbits of complex polynomials
- Showing that for  $f \in \mathbb{Q}[X]$  the function  $f: \mathbb{Q} \rightarrow \mathbb{Q}$  is at most 6-to-1 outside a finite set
- Finding all  $f, g \in \overline{\mathbb{Q}}[X]$  such that  $f(K) \cap g(K)$  is infinite for some number field  $K$
- Determining nonempty finite  $S, T \subset \mathbb{C}$  such that  $P^{-1}(S) \neq Q^{-1}(T)$  for any nonconstant meromorphic  $P, Q$
- Solving  $f^{-1}(U) = g^{-1}(V)$  in  $f, g \in \mathbb{C}[X]$  and infinite compact  $U, V \subset \mathbb{C}$  (Dinh 2005; Pakovich 2008)
- Determining all subvarieties of  $\mathbb{A}^n$  having an endomorphism of the form  $(x_1, \dots, x_n) \mapsto (f_1(x_1), \dots, f_n(x_n))$  where each  $f_i \in \mathbb{C}[X]$  has degree  $\geq 2$  (Medvedev–Scanlon, 2013)
- and several other topics.

## Summary

Solutions of instances of  $f \circ P = g \circ Q$  in polynomials  $f, g$  and meromorphic  $P, Q$  have been applied to:

- Describing intersections of orbits of complex polynomials
- Showing that for  $f \in \mathbb{Q}[X]$  the function  $f: \mathbb{Q} \rightarrow \mathbb{Q}$  is at most 6-to-1 outside a finite set
- Finding all  $f, g \in \overline{\mathbb{Q}}[X]$  such that  $f(K) \cap g(K)$  is infinite for some number field  $K$
- Determining nonempty finite  $S, T \subset \mathbb{C}$  such that  $P^{-1}(S) \neq Q^{-1}(T)$  for any nonconstant meromorphic  $P, Q$
- Solving  $f^{-1}(U) = g^{-1}(V)$  in  $f, g \in \mathbb{C}[X]$  and infinite compact  $U, V \subset \mathbb{C}$  (Dinh 2005; Pakovich 2008)
- Determining all subvarieties of  $\mathbb{A}^n$  having an endomorphism of the form  $(x_1, \dots, x_n) \mapsto (f_1(x_1), \dots, f_n(x_n))$  where each  $f_i \in \mathbb{C}[X]$  has degree  $\geq 2$  (Medvedev–Scanlon, 2013)
- and several other topics.