The Reducibility of $f(X) - g(Y)$ and Polynomial Monodromy

DANNY NEFTIN
based on joint work with
ANGELOT BEHAJAINA AND JOACHIM KÖNIG

Department of Mathematics
Technion - Israel Institute of Technology
Haifa, Israel

Debrecen Number Theory Seminar
May 2026

The curves $f(X) = g(Y)$

For $f, g \in \mathbb{Q}[X]$, consider the curve $f(X) - g(Y) = 0$.
Example: If $g(Y) = Y^2$, then C is a hyperelliptic curve.

Open questions

a) When does $f(X) = g(Y)$ admit infinitely many rational solutions?
b) When does $f(X) = g(Y)$ admit a solution $X = X(z)$, $Y = Y(z) \in \mathbb{C}(z) \setminus \mathbb{C}$?

The curves $f(X) = g(Y)$

For $f, g \in \mathbb{Q}[X]$, consider the curve $f(X) - g(Y) = 0$.
Example: If $g(Y) = Y^2$, then C is a hyperelliptic curve.

Open questions

a) When does $f(X) = g(Y)$ admit infinitely many rational solutions?
b) When does $f(X) = g(Y)$ admit a solution $X = X(z)$, $Y = Y(z) \in \mathbb{C}(z) \setminus \mathbb{C}$?

- Siegel, Faltings, Bilu-Tichy (1929,1983,1999): a) implies $f(X) - g(Y)$ has an irreducible factor of genus ≤ 1.
  Solutions to a) with bounded denominators were classified.

The curves $f(X) = g(Y)$

For $f, g \in \mathbb{Q}[X]$, consider the curve $f(X) - g(Y) = 0$.
Example: If $g(Y) = Y^2$, then C is a hyperelliptic curve.

Open questions

a) When does $f(X) = g(Y)$ admit infinitely many rational solutions?
b) When does $f(X) = g(Y)$ admit a solution $X = X(z), Y = Y(z) \in \mathbb{C}(z) \setminus \mathbb{C}$?

- Siegel, Faltings, Bilu-Tichy (1929,1983,1999): a) implies $f(X) - g(Y)$ has an irreducible factor of genus ≤ 1.
  Solutions to a) with bounded denominators were classified.
- b) implies $f(X) - g(Y)$ has an irreducible factor of genus 0.
- Picard (1883): If $X = X(z), Y = Y(z)$ is a solution in meromorphic functions, then $f(X) - g(Y)$ has an irreducible factor of genus ≤ 1.

Reducibility Problems

The Davenport–Lewis–Schinzel Problem (DLS, 1961)

For what $f, g \in \mathbb{C}[X]$ is $f(X) - g(Y) \in \mathbb{C}[X, Y]$ reducible?

DLS: If $f, g \in \mathbb{C}[X]$ are “generic", then $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is irreducible.

Reducibility Problems

The Davenport–Lewis–Schinzel Problem (DLS, 1961)

For what $f, g \in \mathbb{C}[X]$ is $f(X) - g(Y) \in \mathbb{C}[X, Y]$ reducible?

DLS: If $f, g \in \mathbb{C}[X]$ are “generic", then $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is irreducible.

Fried’s $(2, 3)$-Problem (1987)

Suppose $Y^2 - X^3 + aX + b = 0$ is an elliptic curve$/\mathbb{C}$, $4a^3 + 27b^2 \neq 0$. Can $g(Y)^2 - f(X)^3 - af(X) - b \in \mathbb{C}[X, Y]$ be reducible for some $f, g \in \mathbb{C}[X] \setminus \mathbb{C}$?

Reducibility Problems

The Davenport–Lewis–Schinzel Problem (DLS, 1961)

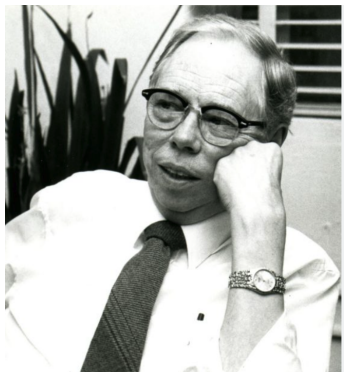
For what $f, g \in \mathbb{C}[X]$ is $f(X) - g(Y) \in \mathbb{C}[X, Y]$ reducible?

DLS: If $f, g \in \mathbb{C}[X]$ are "generic", then $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is irreducible.

Fried's $(2, 3)$-Problem (1987)

Suppose $Y^2 - X^3 + aX + b = 0$ is an elliptic curve/$\mathbb{C}$, $4a^3 + 27b^2 \neq 0$. Can $g(Y)^2 - f(X)^3 - af(X) - b \in \mathbb{C}[X, Y]$ be reducible for some $f, g \in \mathbb{C}[X] \setminus \mathbb{C}$?

Harold Davenport
1907–1969



Donald J. Lewis
1926–2015

Andrzej Schinzel
1937–2021

Related problems

For $f \in \mathbb{Q}[X]$ of degree $d \geq 2$ and $t_0 \in \mathbb{Z}$, the fiber $f^{-1}(t_0)$ is *irreducible*$/\mathbb{Q}$ if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ for any $\alpha \in f^{-1}(t_0) \subseteq \mathbb{C}$, i.e. $f(X) - t_0 \in \mathbb{Q}[X]$ is irreducible.

Hilbert's irreducibility theorem (HIT, 1893)

There exist infinitely many $t_0 \in \mathbb{Z}$ such that $f^{-1}(t_0)$ is irreducible$/\mathbb{Q}$.

Related problems

For $f \in \mathbb{Q}[X]$ of degree $d \geq 2$ and $t_0 \in \mathbb{Z}$, the fiber $f^{-1}(t_0)$ is *irreducible*$/\mathbb{Q}$ if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ for any $\alpha \in f^{-1}(t_0) \subseteq \mathbb{C}$, i.e. $f(X) - t_0 \in \mathbb{Q}[X]$ is irreducible.

Hilbert's irreducibility theorem (HIT, 1893)+Siegel (1923)

There exist infinitely many $t_0 \in \mathbb{Z}$ such that $f^{-1}(t_0)$ is irreducible$/\mathbb{Q}$. In fact, $\mathrm{Red}_f = \{t_0 \in \mathbb{Z} \,|\, f^{-1}(t_0) \text{ is reducible}\}$ is $\mathbb{Z} \cap \bigcup_{i=1}^{r} g_i(\mathbb{Q})$ up to a finite set, for $g_i \in \mathbb{Q}(X)$ s.t. the numerator of $f(X) - g_i(Y)$ in $\mathbb{Q}[X, Y]$ is reducible.

Hilbert–Siegel/Fiber Reducibility Problem ($\leq$ 1974)

For what $f \in \mathbb{Q}[X]$, is $\mathrm{Red}_f = \mathbb{Z} \cap \bigcup_{f=f_1 \circ f_2} f_1(\mathbb{Q})$ up to a finite set?
Here, f_1 runs through left factors of f with $\deg f_1 > 1$.

Related problems

For $f \in \mathbb{Q}[X]$ of degree $d \geq 2$ and $t_0 \in \mathbb{Z}$, the fiber $f^{-1}(t_0)$ is *irreducible*$/\mathbb{Q}$ if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ for any $\alpha \in f^{-1}(t_0) \subseteq \mathbb{C}$, i.e. $f(X) - t_0 \in \mathbb{Q}[X]$ is irreducible.

Hilbert's irreducibility theorem (HIT, 1893)+Siegel (1923)

There exist infinitely many $t_0 \in \mathbb{Z}$ such that $f^{-1}(t_0)$ is irreducible$/\mathbb{Q}$. In fact, $\mathrm{Red}_f = \{t_0 \in \mathbb{Z} \,|\, f^{-1}(t_0) \text{ is reducible}\}$ is $\mathbb{Z} \cap \bigcup_{i=1}^{r} g_i(\mathbb{Q})$ up to a finite set, for $g_i \in \mathbb{Q}(X)$ s.t. the numerator of $f(X) - g_i(Y)$ in $\mathbb{Q}[X, Y]$ is reducible.

Hilbert–Siegel/Fiber Reducibility Problem ($\leq$ 1974)

For what $f \in \mathbb{Q}[X]$, is $\mathrm{Red}_f = \mathbb{Z} \cap \bigcup_{f=f_1 \circ f_2} f_1(\mathbb{Q})$ up to a finite set?
Here, f_1 runs through left factors of f with $\deg f_1 > 1$.

Newly reducible iterates f^n

Given $f \in \mathbb{Q}[X]$ and $n \geq 2$, for what $a \in \mathbb{Q}$ is $f^{-n}(a)$ reducible but $f^{-(n-1)}(a)$ is irreducible? For what $f \in \mathbb{Q}[X]$, is $\mathrm{Red}_{f^n} \setminus \mathrm{Red}_{f^{n-1}}$ infinite?

Examples where $f(X) - g(Y)$ is reducible

Observe: If $f_1(X) - g_1(Y) \in \mathbb{C}[X, Y]$ is reducible, then so is

$$f_1(f_2(X)) - g_1(g_2(Y)) \in \mathbb{C}[X, Y].$$

1. Trivial: $h(X) - h(Y) = (X - Y)H(X, Y)$;

Examples where $f(X) - g(Y)$ is reducible

Observe: If $f_1(X) - g_1(Y) \in \mathbb{C}[X, Y]$ is reducible, then so is

$$f_1(f_2(X)) - g_1(g_2(Y)) \in \mathbb{C}[X, Y].$$

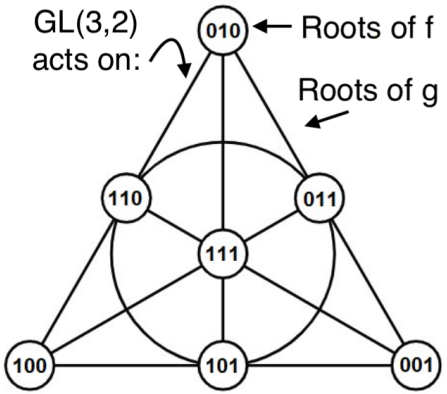
1. Trivial: $h(X) - h(Y) = (X - Y)H(X, Y)$;
2. DLS: $T_4(X) + T_4(Y) = (X^2 - \sqrt{2}XY + Y^2 - 2)(X^2 + \sqrt{2}XY + Y^2 - 2)$; where $T_n(X + 1/X) = X^n + 1/X^n$, so $T_4(X) = X^4 - 4X^2 + 2$.

Examples where $f(X) - g(Y)$ is reducible

Observe: If $f_1(X) - g_1(Y) \in \mathbb{C}[X, Y]$ is reducible, then so is

$$f_1(f_2(X)) - g_1(g_2(Y)) \in \mathbb{C}[X, Y].$$

1. Trivial: $h(X) - h(Y) = (X - Y)H(X, Y)$;
2. DLS: $T_4(X) + T_4(Y) = (X^2 - \sqrt{2}XY + Y^2 - 2)(X^2 + \sqrt{2}XY + Y^2 - 2)$; where $T_n(X + 1/X) = X^n + 1/X^n$, so $T_4(X) = X^4 - 4X^2 + 2$.
3. Cassels-Guy 1968: $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is reducible for some $f, g \in \mathbb{C}[X]$, $\deg f = \deg g \in \{7, 11\}$, $f \neq g \circ \mu$, $\forall \mu \in \mathbb{C}[X]$, $\deg \mu = 1$.

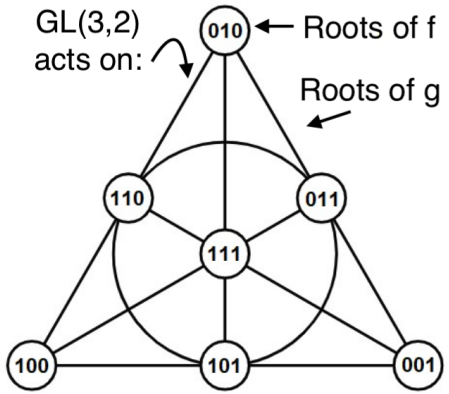


Examples where $f(X) - g(Y)$ is reducible

Observe: If $f_1(X) - g_1(Y) \in \mathbb{C}[X, Y]$ is reducible, then so is

$$f_1(f_2(X)) - g_1(g_2(Y)) \in \mathbb{C}[X, Y].$$

1. Trivial: $h(X) - h(Y) = (X - Y)H(X, Y)$;
2. DLS: $T_4(X) + T_4(Y) = (X^2 - \sqrt{2}XY + Y^2 - 2)(X^2 + \sqrt{2}XY + Y^2 - 2)$; where $T_n(X + 1/X) = X^n + 1/X^n$, so $T_4(X) = X^4 - 4X^2 + 2$.
3. Cassels-Guy 1968: $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is reducible for some $f, g \in \mathbb{C}[X]$, $\deg f = \deg g \in \{7, 11\}$, $f \neq g \circ \mu$, $\forall \mu \in \mathbb{C}[X]$, $\deg \mu = 1$.



4. Fried 1973,1986: If $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is reducible for indecomposable f, g, then $\deg f = \deg g \in \{7, 11, 13, 15, 21, 31\}$.

Is there a minimal example with 4 branch points?

Main Theorem

Theorem (BKN, preprint)

If $f(X) - g(Y) \in \mathbb{C}[X, Y]$ *is reducible, then* $f = \mu \circ f_1 \circ f_2$ *and* $g = \mu \circ g_1 \circ g_2$, *where either* $f_1 = g_1$, *or* $\{f_1, g_1\}$ *is* $\{T_4, -T_4\}$, *or it is one of the pairs of degree* $7, 11, 13, 15, 21$ *or* 31, *for* $f_2, g_2, \mu \in \mathbb{C}[X] \setminus \mathbb{C}$ *with* $\deg \mu = 1$.

Main Theorem

Theorem (BKN, preprint)

If $f(X) - g(Y) \in \mathbb{C}[X,Y]$ *is reducible, then* $f = \mu \circ f_1 \circ f_2$ *and* $g = \mu \circ g_1 \circ g_2$, *where either* $f_1 = g_1$, *or* $\{f_1, g_1\}$ *is* $\{T_4, -T_4\}$, *or it is one of the pairs of degree* $7, 11, 13, 15, 21$ *or* 31, *for* $f_2, g_2, \mu \in \mathbb{C}[X] \setminus \mathbb{C}$ *with* $\deg \mu = 1$.

1. The low degree pairs are given by Cassou-Noguès–Couveignes (1999). A converse holds.
2. This answers also the $(2,3)$-problem. No Cassels monster!
3. A version of the theorem is given over arbitrary fields k of char. 0, allowing $\mu, f_2, g_2 \in \bar{k}[X]$ and replacing T_n by Dickson polynomials.

E.g. $X^4 + 4Y^4 = (X^2 - 2XY + 2Y^2)(X^2 + 2XY + 2Y^2)$.

First applications

Theorem (BKN)

If $f \in \mathbb{Q}[X]$ *is of degree* > 5 *with no composition factors of degree* 2 *or* 4, *then* $\mathrm{Red}_f = (\bigcup f_1(\mathbb{Q}) \cap \mathbb{Z}) \cup$ *finite set, where* f_1 *runs over left factors* $f = f_1 \circ f_2$.

First applications

Theorem (BKN)

If $f \in \mathbb{Q}[X]$ *is of degree* > 5 *with no composition factors of degree* 2 *or* 4, *then* $\mathrm{Red}_f = (\bigcup f_1(\mathbb{Q}) \cap \mathbb{Z}) \cup$ *finite set, where* f_1 *runs over left factors* $f = f_1 \circ f_2$.

Corollary (BKN)

Let $n \geq 2$ *and* $f \in \mathbb{Q}[X]$ *be of degree* > 1 *with no composition factors of degree* 2 *or* 4. *Then* $\mathrm{Red}_{f^n} \setminus \mathrm{Red}_f$ *is finite.*

First applications

Theorem (BKN)

If $f \in \mathbb{Q}[X]$ *is of degree* > 5 *with no composition factors of degree* 2 *or* 4, *then* $\mathrm{Red}_f = (\bigcup f_1(\mathbb{Q}) \cap \mathbb{Z}) \cup$ *finite set, where* f_1 *runs over left factors* $f = f_1 \circ f_2$.

Corollary (BKN)

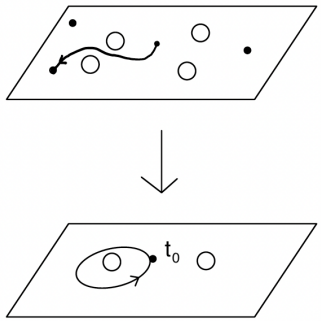
Let $n \geq 2$ *and* $f \in \mathbb{Q}[X]$ *be of degree* > 1 *with no composition factors of degree* 2 *or* 4. *Then* $\mathrm{Red}_{f^n} \setminus \mathrm{Red}_f$ *is finite.*

Corollary (BKN)

Let f, g *have no common left factor of degree* > 1. *If* $f(X) - g(Y) \in \mathbb{C}[X, Y]$ *is reducible and* $f(X(z)) = g(Y(z))$ *for* $X = X(z), Y = Y(z) \in \mathbb{C}(z) \setminus \mathbb{C}$, *then* $f = \mu \circ f_1 \circ \lambda_1$, $g = \mu \circ g_1 \circ \lambda_2$, *where* $\{f_1, g_1\}$ *is either* $\{T_{2^n}, -T_{2^m}\}$, $m, n \geq 2$, *or* $\deg f_1 = \deg g_1 \in \{7, 13\}$, *for* $\mu, \lambda_1, \lambda_2 \in \mathbb{C}[X]$ *of degree* 1.

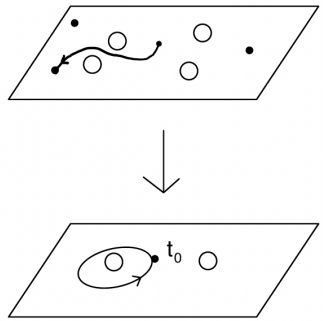
Monodromy groups

Let $f \in \mathbb{C}[X]$ be of degree $d \geq 2$. $\mathrm{Mon}(f)$ is the image of the action of the fundamental group on $f^{-1}(t_0)$, or $\mathrm{Mon}(f) = \mathrm{Gal}(f(X) - t, \mathbb{C}(t)) \leq \mathrm{Sym}(R_f) \cong S_d$, where $R_f = \{\text{Roots of } f(X) - t\}$.



Monodromy groups

Let $f \in \mathbb{C}[X]$ be of degree $d \geq 2$. $\mathrm{Mon}(f)$ is the image of the action of the fundamental group on $f^{-1}(t_0)$, or $\mathrm{Mon}(f) = \mathrm{Gal}(f(X) - t, \mathbb{C}(t)) \leq \mathrm{Sym}(R_f) \cong S_d$, where $R_f = \{\text{Roots of } f(X) - t\}$.



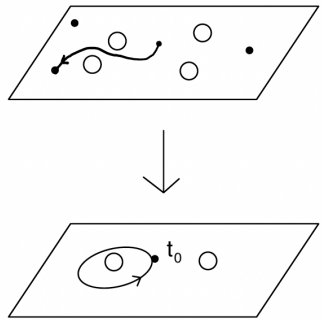
Observation

1) $\Omega := \mathrm{SplittingFld}(f(X) - t, \mathbb{C}(t)) = \mathrm{SplittingFld}(g(X) - t, \mathbb{C}(t))$.
2) $G = \mathrm{Gal}(\Omega/\mathbb{C}(t))$ acts transitively on R_f and on R_g.
3) $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is irreducible iff G acts on $R_f \times R_g$ transitively.

Example: If $G = \mathrm{GL}(3, 2)$, and R_f, R_g are lines and hyperplanes in $\mathbb{F}_2^3$, resp., then G acts on $R_f \times R_g$ intransitively.

Monodromy groups

Let $f \in \mathbb{C}[X]$ be of degree $d \geq 2$. $\mathrm{Mon}(f)$ is the image of the action of the fundamental group on $f^{-1}(t_0)$, or $\mathrm{Mon}(f) = \mathrm{Gal}(f(X) - t, \mathbb{C}(t)) \leq \mathrm{Sym}(R_f) \cong S_d$, where $R_f = \{\text{Roots of } f(X) - t\}$.



Observation

1) $\Omega := \mathrm{SplittingFld}(f(X) - t, \mathbb{C}(t)) = \mathrm{SplittingFld}(g(X) - t, \mathbb{C}(t))$.
2) $G = \mathrm{Gal}(\Omega/\mathbb{C}(t))$ acts transitively on R_f and on R_g.
3) $f(X) - g(Y) \in \mathbb{C}[X, Y]$ is irreducible iff G acts on $R_f \times R_g$ transitively.

Example: If $G = \mathrm{GL}(3, 2)$, and R_f, R_g are lines and hyperplanes in $\mathbb{F}_2^3$, resp., then G acts on $R_f \times R_g$ intransitively.

Problem

What can $G = \mathrm{Mon}(f)$ be for a polynomial $f \in \mathbb{C}[X]$?

The Monodromy of a Polynomial

Theorem (Schur, Ritt, Burnside, Feit, Müller 95)

Let $f \in \mathbb{C}[x] \setminus \mathbb{C}$ be indecomposable of $d := \deg f \geq 2$. Then $\Gamma := \mathrm{Mon}(f)$ is either solvable or almost-simple. Moreover, if $\Gamma \neq A_d, S_d$, then either $f = \mu_1 \circ x^d \circ \mu_2$ or $\mu_1 \circ T_d \circ \mu_2$ for $\mu_1, \mu_2 \in \mathbb{C}[X]$ of degree 1 or f is in an explicit list with $d \leq 31$.

To end

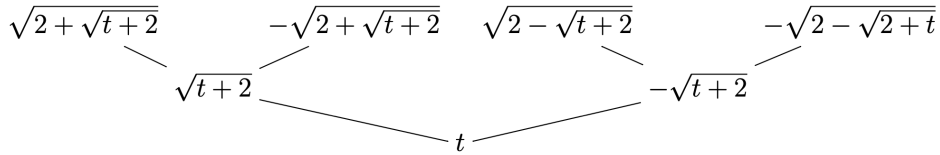
The Monodromy of a Polynomial

Theorem (Schur, Ritt, Burnside, Feit, Müller 95)

Let $f \in \mathbb{C}[x] \setminus \mathbb{C}$ be indecomposable of $d := \deg f \geq 2$. Then $\Gamma := \mathrm{Mon}(f)$ is either solvable or almost-simple. Moreover, if $\Gamma \neq A_d, S_d$, then either $f = \mu_1 \circ x^d \circ \mu_2$ or $\mu_1 \circ T_d \circ \mu_2$ for $\mu_1, \mu_2 \in \mathbb{C}[X]$ of degree 1 or f is in an explicit list with $d \leq 31$.

Remark: If $f = g \circ h$, $d = \deg g = \deg h$, then $\mathrm{Mon}(f) \leq S_d \wr S_d = S_d^d \rtimes S_d$.

E.g. $\mathrm{Mon}(T_2 \circ T_2)$ acts on:



To end

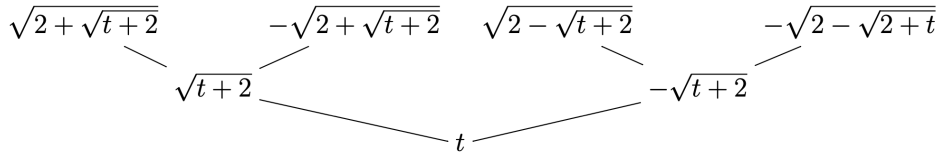
The Monodromy of a Polynomial

Theorem (Schur, Ritt, Burnside, Feit, Müller 95)

Let $f \in \mathbb{C}[x] \setminus \mathbb{C}$ be indecomposable of $d := \deg f \geq 2$. Then $\Gamma := \mathrm{Mon}(f)$ is either solvable or almost-simple. Moreover, if $\Gamma \neq A_d, S_d$, then either $f = \mu_1 \circ x^d \circ \mu_2$ or $\mu_1 \circ T_d \circ \mu_2$ for $\mu_1, \mu_2 \in \mathbb{C}[X]$ of degree 1 or f is in an explicit list with $d \leq 31$.

Remark: If $f = g \circ h$, $d = \deg g = \deg h$, then $\mathrm{Mon}(f) \leq S_d \wr S_d = S_d^d \rtimes S_d$.

E.g. $\mathrm{Mon}(T_2 \circ T_2)$ acts on:



Theorem (König–N–Rosenberg)

Suppose $f = f_1 \circ \cdots \circ f_r$ for $f_1, \ldots, f_r \in \mathbb{C}[x]$ of degree ≥ 5 with $\mathrm{Mon}(f_i) \cong S_{d_i}$, then $\mathrm{Mon}(f) \supseteq A_{d_r} \wr \cdots \wr A_{d_1}$.

In contrast, $f(X) = X^p \circ h_2(X) = h_1(X) \circ X^p \Rightarrow \mathrm{Mon}(f) = C_p \times \mathrm{Mon}(h_1)$!

To end

Proof - Main Ideas

1. Assume (f, g) is a minimal counterexample and write $f = h \circ f_{r-1} \circ f_r$ for indecomposable $f_{r-1}, f_r \in \mathbb{C}[X]$. Then f_r is a unique right factor ($f = u \circ v \Rightarrow v = v' \circ f_r$).

To end

Proof - Main Ideas

1. Assume (f, g) is a minimal counterexample and write $f = h \circ f_{r-1} \circ f_r$ for indecomposable $f_{r-1}, f_r \in \mathbb{C}[X]$. Then f_r is a unique right factor ($f = u \circ v \Rightarrow v = v' \circ f_r$).
2. Reduction to case where $\mathrm{Mon}(f) \cong \mathrm{Mon}(g)$ is solvable.

To end

Proof - Main Ideas

1. Assume (f, g) is a minimal counterexample and write $f = h \circ f_{r-1} \circ f_r$ for indecomposable $f_{r-1}, f_r \in \mathbb{C}[X]$. Then f_r is a unique right factor ($f = u \circ v \Rightarrow v = v' \circ f_r$).
2. Reduction to case where $\mathrm{Mon}(f) \cong \mathrm{Mon}(g)$ is solvable.
3. Key observation: Consider $K = \ker(\mathrm{Mon}(f) \to \mathrm{Mon}(h \circ f_{r-1}) \leq \Gamma^d$, where $\Gamma = \mathrm{Mon}(f_r)$ and $d = \deg(h \circ f_{r-1})$. Then K is diagonal, i.e. the projections $K \to \Gamma$ are injective.

To end

Proof - Main Ideas

1. Assume (f,g) is a minimal counterexample and write $f = h \circ f_{r-1} \circ f_r$ for indecomposable $f_{r-1}, f_r \in \mathbb{C}[X]$. Then f_r is a unique right factor ($f = u \circ v \Rightarrow v = v' \circ f_r$).
2. Reduction to case where $\mathrm{Mon}(f) \cong \mathrm{Mon}(g)$ is solvable.
3. Key observation: Consider $K = \ker(\mathrm{Mon}(f) \to \mathrm{Mon}(h \circ f_{r-1}) \leq \Gamma^d$, where $\Gamma = \mathrm{Mon}(f_r)$ and $d = \deg(h \circ f_{r-1})$. Then K is diagonal, i.e. the projections $K \to \Gamma$ are injective.
4. Since $f_{r-1} \circ f_r$ has no Ritt step, $\Gamma_2 := \mathrm{Mon}(f_{r-1} \circ f_r)$ has to be *large*, i.e. contains an index $p = \deg f_r$ subgroup of $C_p^{d'}$ where $d' = \deg f_{r-1}$.

To end

Proof - Main Ideas

1. Assume (f,g) is a minimal counterexample and write $f = h \circ f_{r-1} \circ f_r$ for indecomposable $f_{r-1}, f_r \in \mathbb{C}[X]$. Then f_r is a unique right factor ($f = u \circ v \Rightarrow v = v' \circ f_r$).
2. Reduction to case where $\mathrm{Mon}(f) \cong \mathrm{Mon}(g)$ is solvable.
3. Key observation: Consider $K = \ker(\mathrm{Mon}(f) \to \mathrm{Mon}(h \circ f_{r-1}) \leq \Gamma^d$, where $\Gamma = \mathrm{Mon}(f_r)$ and $d = \deg(h \circ f_{r-1})$. Then K is diagonal, i.e. the projections $K \to \Gamma$ are injective.
4. Since $f_{r-1} \circ f_r$ has no Ritt step, $\Gamma_2 := \mathrm{Mon}(f_{r-1} \circ f_r)$ has to be *large*, i.e. contains an index $p = \deg f_r$ subgroup of $C_p^{d'}$ where $d' = \deg f_{r-1}$.
5. The image of $\ker(\mathrm{Mon}(f) \to \mathrm{Mon}(h))$ in Γ_2 cannot be diagonal, unless $p = 2, 3$.

To end

Proof - Main Ideas

1. Assume (f,g) is a minimal counterexample and write $f = h \circ f_{r-1} \circ f_r$ for indecomposable $f_{r-1}, f_r \in \mathbb{C}[X]$. Then f_r is a unique right factor ($f = u \circ v \Rightarrow v = v' \circ f_r$).
2. Reduction to case where $\mathrm{Mon}(f) \cong \mathrm{Mon}(g)$ is solvable.
3. Key observation: Consider $K = \ker(\mathrm{Mon}(f) \to \mathrm{Mon}(h \circ f_{r-1}) \leq \Gamma^d$, where $\Gamma = \mathrm{Mon}(f_r)$ and $d = \deg(h \circ f_{r-1})$. Then K is diagonal, i.e. the projections $K \to \Gamma$ are injective.
4. Since $f_{r-1} \circ f_r$ has no Ritt step, $\Gamma_2 := \mathrm{Mon}(f_{r-1} \circ f_r)$ has to be *large*, i.e. contains an index $p = \deg f_r$ subgroup of $C_p^{d'}$ where $d' = \deg f_{r-1}$.
5. The image of $\ker(\mathrm{Mon}(f) \to \mathrm{Mon}(h))$ in Γ_2 cannot be diagonal, unless $p = 2, 3$.
6. 3-step analogue, and then a separate argument when f and g admit right factors of degree 8 and 16.

To end

Further questions

Fiber Reducibility Problem

For what f, is $\mathrm{Red}_f(\mathbb{Q}) \setminus \bigcup_{f_1} f_1(\mathbb{Q})$ is infinite?

When is there an effective solution?

Further questions

Fiber Reducibility Problem

For what f, is $\mathrm{Red}_f(\mathbb{Q}) \setminus \bigcup_{f_1} f_1(\mathbb{Q})$ is infinite?

When is there an effective solution?

Davenport's Problem (1968)

For what $f, g \in \mathbb{Q}[X] \setminus \mathbb{Q}$, is $f(\mathbb{F}_p) = g(\mathbb{F}_p)$ for all but finitely many primes p?

For such (Kronecker conjugate) pairs, write $f \equiv_{\mathbb{Q}} g$.

Further questions

Fiber Reducibility Problem

For what f, is $\mathrm{Red}_f(\mathbb{Q}) \setminus \bigcup_{f_1} f_1(\mathbb{Q})$ is infinite?

When is there an effective solution?

Davenport's Problem (1968)

For what $f, g \in \mathbb{Q}[X] \setminus \mathbb{Q}$, is $f(\mathbb{F}_p) = g(\mathbb{F}_p)$ for all but finitely many primes p?

For such (Kronecker conjugate) pairs, write $f \equiv_{\mathbb{Q}} g$.

Examples for $f \equiv_{\mathbb{Q}} g$

1. $f(X) = g(\mu(X))$ for $\mu \in \mathbb{Q}[X]$;
2. $f = h(x^8)$ and $g = h(16x^8)$ for $h \in \mathbb{Q}[x]$.

Remark: $f \equiv_{\mathbb{Q}} g$ implies $f(X) - g(Y) \in \mathbb{Q}[X, Y]$ is reducible.

Thank you!

Thanks for attending!

The slides will appear on the seminar's webpage.

Thank you!

Thanks for attending!

The slides will appear on the seminar's webpage.

Back