Composite polynomials as sums of powers of two fixed polynomials

Dijana Kreso
University of Salzburg

Representation Theory XIX
June 25, 2025

Central question

Work in progress - with Clemens Fuchs (Univ. of Salzburg):
Composite polynomials expressible as sums of powers of two fixed polynomials:

$$g(h(x)) = ap(x)^n + bq(x)^m + c,$$

where p and q are fixed nonconstant complex polynomials, $a, b, c \in \mathbb{C}$ and $n, m \in \mathbb{N}_0$.

Central question

Work in progress - with Clemens Fuchs (Univ. of Salzburg):
Composite polynomials expressible as sums of powers of two fixed polynomials:

$$g(h(x)) = ap(x)^n + bq(x)^m + c,$$

where p and q are fixed nonconstant complex polynomials, $a, b, c \in \mathbb{C}$ and $n, m \in \mathbb{N}_0$.

Proposition (Fried–Schinzel 1972)

Assume that complex polynomials g and h satisfy

$$g(h(x)) = ax^n + bx^m + c, \quad n > m \geq 1, \ a, b, c \in \mathbb{C}, \ ab \neq 0.$$

Then there exists a liner polynomial $\ell \in \mathbb{C}[x]$ s.t. either

$$g(x) = \ell(x), \quad h(x) = \ell^{(-1)} \circ (ax^n + bx^m + c),$$

or

$$g(x) = \left(a_1 x^{n_1/k} + a_2 x^{n_2/k} + a_3\right) \circ \ell^{(-1)}, \quad h(x) = \ell \circ x^k,$$

for some $k \mid \gcd(n_1, n_2)$.

If $\ell(x) = ax + b$, then $\ell^{(-1)}(x) = \frac{1}{a}x - \frac{b}{a}$.

Ritt's theorems

Theorem (Ritt's First Theorem 1922)

If $f \in \mathbb{C}[x]$ and $\deg f > 1$, then any complete decomposition of $f(x)$ can be obtained from any other through finitely many steps, where each step consists of replacing two adjacent indecomposables by two others with the same composition.

Ritt's theorems

Theorem (Ritt's First Theorem 1922)

If $f \in \mathbb{C}[x]$ and $\deg f > 1$, then any complete decomposition of $f(x)$ can be obtained from any other through finitely many steps, where each step consists of replacing two adjacent indecomposables by two others with the same composition.

Ritt then solved the equation

$$a \circ b = c \circ d,$$

in indecomposable complex polynomials a, b, c, d (Ritt's Second Theorem 1922).

The only solutions are

- the trivial $a \circ b = a \circ b$ (meaning $c \circ d = (a \circ \ell) \circ (\ell^{(-1)} \circ b)$)
- and the nontrivial that arise from the following identities through composing with linears

$$x^n \circ x^s P(x^n) = x^s P(x)^n \circ x^n, \quad T_n(x) \circ T_m(x) = T_m(x) \circ T_n(x),$$

  where $P(x) \in \mathbb{C}[x]$ and $T_n(x)$ is the n-th Chebyshev polynomial of the first kind:

$$T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x), \quad T_0(x) = 1, \ T_1(x) = x.$$

To that end:

- cyclic polynomials: $\ell(x) \circ x^m \circ \mu(x)$, $m \geq 2$,
- dihedral polynomials: $\ell(x) \circ T_m(x) \circ \mu(x)$, $m \geq 3$, where ℓ, μ are linears.

Applications to Diopantine equations

Theorem (Péter, Pintér & Schinzel 2011)

The Diophantine equation

$$a_1 x^{m_1} + a_2 x^{m_2} + a_3 = b_1 y^{n_1} + b_2 y^{n_2},$$

where

- $m_1 > m_2 > 0$, $n_1 > n_2 > 0$, $\gcd(m_1, m_2) = 1 = \gcd(n_1, n_2)$,
- $a_i, b_j \in \mathbb{Q}$ and $a_1 a_1 b_1 b_2 \neq 0$,

and either

- $m_1 > n_1 \geq 3$,
- or $m_1 = n_1 \geq 3$ and $m_2 \geq n_2$,

has infinitely many rational solutions x, y with a bounded denominator iff either

- $m_1 = n_1$, $m_2 = n_2$, $a_1 = b_1 t^{m_1}$, $a_2 = b_2 t^{m_2}$, $c = 0$, $t \in \mathbb{Q}$,
- or $m_1 = n_1 = 3$, $m_2 = n_2 = 2$, $a_1^2 b_3 + a_2^3 b_1^2 = 0$, $c = -\frac{4 a_2^3}{27 a_1^2}$,
- or $m_1 = n_1 = 3$, $m_2 = 2$, $n_2 = 1$, $26 a_1^4 b_2^3 + a_2^6 b_1 = 0$, $c = -\frac{3 a_1^2 b_2^3 + a_2^3 b_2^2}{3 a_2^3 b_1}$.

Case $n = m$ and Zannier's results

Theorem (K. 2022; Fuchs-Karolus & K. 2017)

For complex polynomials p and q, let $g(x), h(x) \in \mathbb{C}[x]$ be such that

$$g(h(x)) = p(x)^n + q(x)^n,$$

for some $n \geq 0$. Assuming h is indecomposable and neither cyclic nor dihedral, we have that

- either $p(x), q(x) \in \mathbb{C}[h(x)]$
- or $\deg g \leq C$ for a constant $C = C(p, q) > 0$, independent of n.

Theorem (Zannier 2007)

Let $f \in \mathbb{C}[x]$ have $\ell > 0$ nonconstant terms. Assume $f = g \circ h$, where h is not of the form $ax^k + b$. Then $\deg g \leq 2\ell(\ell - 1)$.

Theorem (Zannier 2008, conjectured by Schinzel 1987)

There exists a (computable) function B on $\mathbb{N}$ such that if $g, h \in \mathbb{C}[x]$ are nonconstant and $f = g \circ h$ has ℓ terms, then h has at most $B(\ell)$ terms.

Zannier's method

Theorem (Zannier 2007)

Let $f \in \mathbb{C}[x]$ have $\ell > 0$ nonconstant terms. Assume $f = g \circ h$, where h is not of shape $ax^k + b$. Then $\deg g \leq 2\ell(\ell - 1)$.

The central component of the proof is the following theorem.

Theorem (Brownawell-Masser 1986)

Let $F/\mathbb{C}$ be a function field of one variable of genus g. Moreover, for a finite set S of discrete valuations, let $u_1, \ldots, u_n$ be S-units, which are not all constant, such that

$$1 + u_1 + u_2 + \ldots + u_n = 0,$$

and that no proper subsum of the left hand side vanishes. Then we have

$$\max_{i=1,\ldots,n} \mathcal{H}(u_i) \leq \binom{n}{2}(|S| + \max(0, 2g - 2)). \tag{2}$$

$$\mathcal{H}(f) = -\sum_{\nu} \min(0, \nu(f)). \tag{3}$$

The sum is taken over all discrete valuations ν on F. The set of S-units in F is

$$\mathcal{O}_S^* = \{f \in F : \nu(f) = 0 \text{ for all } \nu \notin S\}.$$

Back to our problem

Assume that for fixed nonconstant complex polynomials p and q there exist such g and h s.t.

$$g(h(x)) = ap(x)^n + bq(x)^m + c,$$

for some $a, b, c \in \mathbb{C}$ and $n, m \in \mathbb{N}$.

- Assume $\deg h \geq 2$.
- For t transcedental over $\mathbb{C}$ let x be a root of of $h(X) - t$ over $\mathbb{C}(t)$, s.t. $h(x) = t$.
- By Gauss's Lemma $h(X) - t$ is irreducible and therefore also separable over $\mathbb{C}(t)$.
- Let $y \neq x$ be a conjugate of x over $\mathbb{C}(h(x))$, so that $h(x) = h(y)$.
- Then also $g(h(x)) = g(h(y))$ and hence

$$ap(x)^n + bq(x)^m = ap(y)^n + bq(y)^m.$$

We may apply Brownawell and Masser's lemma by rewriting the equation as follows

$$1 + \frac{bq(x)^m}{ap(x)^n} - \frac{ap(y)^n}{ap(x)^n} - \frac{bq(y)^m}{ap(x)^n} = 0.$$

- Let S be a set of discrete valuations on $\mathbb{C}(x, y)$ s.t. $\frac{bq(x)^m}{ap(x)^n}, \frac{ap(y)^n}{ap(x)^n}, \frac{bq(y)^m}{ap(x)^n}$ are S-units.
- Let $d = [\mathbb{C}(x, y) : \mathbb{C}(x)]$.
- We can show $|S| \leq c(p, q)d$ for a constant $c(p, q)$ depending only on p and q.
- We can bound d by $\deg h - 1$. We can bound g from above by $(d - 1)(d - 2)/2$.

Thank you for the attention.