Extensions of the theorem of Julia-Ritt for polynomials.

Rob Tijdeman

Leiden University

Joint work with Lajos Hajdu

Debrecen Number Theory Seminar
13 March 2026

Definitions and notation

Let $f, g \in \mathbb{C}[z]$. (All polynomials are in $\mathbb{C}[z]$). We write $f \circ g$ for $f(g)$.
We call f, g *commuting* if $f \circ g = g \circ f$.
We write $f^{[s]}$ for the s-fold iterate of f under composition.
Let ℓ be a linear (polynomial) and $\ell^{[-1]}$ the composite inverse of ℓ.
Thus $\ell^{[-1]} \circ \ell = \ell \circ \ell^{[-1]} = z$. ($z$ is the composition identity.)
If $f \circ g = g \circ f$, then
$(\ell^{[-1]} \circ f \circ \ell) \circ (\ell^{[-1]} \circ g \circ \ell) = (\ell^{[-1]} \circ g \circ \ell) \circ (\ell^{[-1]} \circ f \circ \ell)$ for any linear ℓ.
So, if f and g commute, then also $\ell^{[-1]} \circ f \circ \ell$ and $\ell^{[-1]} \circ g \circ \ell$.
f and f^* are called *similar* if $f^* = \ell^{[-1]} \circ f \circ \ell$ for some linear ℓ.

The *normalized Chebyshev polynomials of the first kind*, T_n, are defined by

$$T_0 = 2, \ T_1 = z, \ T_n = zT_{n-1} - T_{n-2} \ \ (n = 2, 3, \ldots).$$

A *monomial* is a polynomial of the form az^n with $a \in \mathbb{C}$ and $n \in \mathbb{Z}_{\geq 0}$.

Theorem of Julia-Ritt

Let m, n be positive integers. It is true that
$T_n \circ T_m = T_{nm} = T_m \circ T_n$,
$z^n \circ z^m = z^{nm} = z^m \circ z^n$,
$f^{[n]} \circ f^{[m]} = f^{[n+m]} = f^{[m]} \circ f^{[n]}$.
This gives three distinct types of commuting pairs.

Theorem (of Julia-Ritt (short version))

Let $f, g \in \mathbb{C}[z]$ be of degree ≥ 2 such that $f \circ g = g \circ f$.
Then one of the following holds.
(i) f and g are similar, via the same linear, to Chebyshev polynomials.
(ii) f and g are similar, via the same linear, to monomials.
(iii) There exist positive integers m and n such that $f^{[m]} = g^{[n]}$.

The commuting polynomial theorem of Julia

Theorem (of Julia-Ritt (short version))

Let both P and Q be of degree ≥ 2 *such that* $f \circ g = g \circ f$.
Then one of the following holds.
(i) f and g are similar, via the same linear, to Chebyshev polynomials.
(ii) f and g are similar, via the same linear, to monomials.
(iii) There exist positive integers m and n such that $f^{[m]} = g^{[n]}$.

Theorem (Julia, 1922)

The only polynomials which satisfy $f \circ g = g \circ f$ *are such that either there are positive integers* m, n *such that* $f^{[m]} = g^{[n]}$
or they are similar by the same linear to one of the forms:
1) $z^m, \rho z^n$ *with* $\rho \in \mathbb{C}, \rho^{m-1} = 1$,
2) $\cos(mu + \varepsilon_1 \pi),\ \cos(nu + \varepsilon_2 \pi)$
$(z = \cos u; m, n \in \mathbb{Z}_{>0}; \varepsilon_1, \varepsilon_2 \in \{0, 1\})$,
where $m\varepsilon_2 + \varepsilon_1$ *and* $n\varepsilon_1 + \varepsilon_2$ *have the same parity.*

The theorem of Julia-Ritt

Theorem (Julia, 1922)

The only polynomials which satisfy $f \circ g = g \circ f$ are such that either there are positive integers m, n such that $f^{[m]} = g^{[n]}$ or they are similar by the same linear to one of the forms:
$z^m, \rho z^n$ *with* $\rho \in \mathbb{C}, \rho^{m-1} = 1$,
$\cos(mu + \varepsilon_1 \pi), \ \cos(nu + \varepsilon_2 \pi)$.

Theorem (Ritt, 1923)

If f and g are commuting non-linear polynomials which do not come from the multiplication formulas of e^z and $\cos z$, then there exists a linear ℓ and a polynomial $G(z) = zR(z^r)$ such that
$f = \ell^{[-1]} \circ \rho_1 G^{[n]} \circ \ell, \ \ g = \ell^{[-1]} \circ \rho_2 G^{[m]} \circ \ell$,
where ρ_1, ρ_2 are r-th roots of unity and $m, n \in \mathbb{Z}_{>0}$.

This means that $\rho_1 z$ and G as well as $\rho_2 z$ and G are commuting.

Ritt's decomposition theory, after Zieve-Mueller (2008)

A polynomial f of degree > 1 is called *indecomposable* if it cannot be written as the composition of polynomials of strictly lower degrees.

A *complete decomposition* of f is a finite sequence $(f_1, f_2, \dots, f_r)$ of indecomposable polynomials such that $f = f_1 \circ f_2 \circ \dots \circ f_r$.

Theorem (Ritt's basic decomposition theorem)

Let $\deg(f) > 1$. If $\mathcal{U}$ and $\mathcal{V}$ are complete decompositions of f, then card($\mathcal{U}$) = card($\mathcal{V}$) and the multiset of degrees is the same.

Let $(u_1, \dots, u_r)$ and $(v_1, \dots, v_r)$ be complete decompositions of f. If there is an i such that $u_j = v_j$ for $j \notin \{i, i+1\}$, $\gcd(\deg(u_i), \deg(v_i)) = 1$, and $u_i \circ u_{i+1} = v_i \circ v_{i+1}$, we call it a *Ritt switch*.

Theorem (Ritt's first decomposition theorem)

Let $\deg(f) > 1$. If $\mathcal{U}$ and $\mathcal{V}$ are complete decompositions of f, then there is a finite sequence of Ritt switches which transforms $\mathcal{U}$ into $\mathcal{V}$.

Ritt's Second decomposition theorem (after ZM)

(Possible Ritt switches) Suppose $P \circ Q = R \circ S$ and $\gcd(\deg(P), \deg(R)) = \gcd(\deg(Q), \deg(S)) = 1$.
Hence $\deg(P) = \deg(S), \quad \deg(Q) = \deg(R)$.
Then there are linears ℓ_j $(j = 1, 2, 3, 4)$ such that

$$(\ell_1 \circ P \circ \ell_2^{[-1]}, \ell_2 \circ Q \circ \ell_3, \ell_1 \circ R \circ \ell_4^{[-1]}, \ell_4 \circ S \circ \ell_3^{[-1]})$$

has one of the forms

$$(T_n, T_m, T_m, T_n),$$

$$(z^n, z^s G(z^n), z^s G(z)^n, z^n),$$

$$(z^s G(z)^n, z^n, z^n, z^s G(z^n)),$$

where $m, n > 0$ are coprime, $s \geq 0$ is coprime to n, and $G \in \mathbb{C}[z]]$.

Note that $z^s G(z)^n \circ z^n = z^{ns} G(z^n)^n, \quad z^n \circ z^s G(z^n) = z^{ns} G(z^n)^n$.

Generalizations of the Ritt theorems

Ritt's First Theorem was proved by Ritt in 1922 for $\mathbb{C}$,
by Engstrom in 1941 for char $K = 0$,
by Schinzel in 1980 for fields K with $\deg f$ not divisible by char K .
Dorey and Whaples (1974) gave an example that the statement is wrong when char $K \mid \deg f$.

Ritt's Second Theorem was proved by Ritt in 1922 for $\mathbb{C}$,
by Levi in 1942 for char $K = 0$ and P, Q, R, S indecomposable,
by Dorey and Whaples in 1974 for char $K > \max(\deg(f), \deg(g))$ and P, Q, R, S indecomposable,
and without the indecomposability condition by Schinzel in 1980.

Application 1: Factorization

Question: How to decompose f into $g \circ h$?
E.g. fast and simple algorithm by Kozen and Landau (1989)

Application (due to Barton and Zippel, 1985):
Factorize $f = z^6 + 6z^4 + z^3 + 9z^2 + 3z + 5$.

First, use decomposition algorithm:
$g = z^2 + z - 5, \; h = z^3 + 3z, \quad f = g \circ h$.
Next factorize g for its roots α, then factorize $h - \alpha$ for the roots α of g.

Used in computer algebra systems such as MACSYMA, MAPLE and SCRATCHPAD.

Application 2: Theorem of Bilu-Tichy (2000)

Let $f, g \in \mathbb{Q}[x]$ be non-constant. Then these statements are equivalent:

(A) Equation $f(x) = g(y)$ has infinitely many solutions in $\mathbb{Q}$ with bounded denominator.

(B) $f = \phi \circ f_1 \circ \ell_1$, $g = \phi \circ g_1 \circ \ell_2$ with $\phi \in \mathbb{Q}[x]$, $\ell_1, \ell_2 \in \mathbb{Q}[x]$ linears, (f_1, g_1) is a standard pair such that $f_1(x) = g_1(y)$ has infinitely many solutions in $\mathbb{Q}$ with bounded denominator.

Standard pairs are essentially:
1. $(x^m, ax^r p(x)^m)$, 2. $(x^2, (ax^2 + b)p(x)^2)$,
3. $(D_m(x, a^n), D_n(x, a^m))$, 4. $(a^{-m/2} D_m(x, a), -b^{-n/2} D_n(x, b))$,
5. $((ax^2 - 1)^3, 3x^4 - 4x^3)$.

Here $D_m(x, a)$ is the m-th Dickson polynomial, $D_m(x, 1) = T_m$.

The equation $P \circ Q = R \circ S$, due to Ritt, cf. ZM Lemma 2.8

Theorem

Let $P, Q, R, S \in \mathbb{C}[z] \setminus \mathbb{C}$ *satisfy* $P \circ Q = R \circ S$.
Then there exist $F, H, P_1, Q_1, R_1, S_1 \in \mathbb{C}[z]$ *such that*

$$P = F \circ P_1, \; R = F \circ R_1, \;\; \deg(F) = \gcd(\deg(P), \deg(R)).$$

$$Q = Q_1 \circ H, \; S = S_1 \circ H, \;\; \deg(H) = \gcd(\deg(Q), \deg(S)).$$

$$P_1 \circ Q_1 = R_1 \circ S_1.$$

The equation $P \circ Q = R \circ S$, Corollary

Theorem

Let $P, Q, R, S \in \mathbb{C}[z] \setminus \mathbb{C}$ satisfy $P \circ Q = R \circ S$.
Then there exist $F, H, P_1, Q_1, R_1, S_1 \in \mathbb{C}[z]$ such that

$$P = F \circ P_1,\ \ R = F \circ R_1,\ \ \deg(F) = \gcd(\deg(P), \deg(R)).$$

$$Q = Q_1 \circ H,\ \ S = S_1 \circ H,\ \ \deg(H) = \gcd(\deg(Q), \deg(S)).$$

$$P_1 \circ Q_1 = R_1 \circ S_1.$$

Corollary

If $\deg(R) \mid \deg(P)$, *then* $P = R \circ P_1$ *for some* P_1.

If $\deg(S) \mid \deg(Q)$, *then* $Q = Q_1 \circ S$ *for some* Q_1

If $\deg(P) = \deg(R)$, *then* $P = R \circ \ell,\ Q = \ell^{[-1]} \circ S$ *for some linear* ℓ.

The equation $f \circ g = g \circ h$ with $\deg(f) = 1$ (HT,arXiv)

Theorem

Let $a, b, c, d \in \mathbb{C}$ *with* $ac \neq 0$ *and* $g \in \mathbb{C}[z]$*,with* $\deg(g) = n > 1$ *such that* $(az + b) \circ g = g \circ (cz + d)$*. Then* $a = c^n$ *and one of the following options holds.*

$$\text{A)}\ \ (a, b, c, d) = (1, 0, 1, 0).$$

B) If $c \neq 1$*, but* c *is a* t*-th root of unity, then*

$$g = \sum_{j=0}^{(n-1)/t} e_j \left(z + \frac{d}{c-1}\right)^{n-jt} - \frac{b}{a-1}.$$

C) If c *is not a root of unity, then for some* $e_0 \in \mathbb{C}$

$$g = e_0 \left(z + \frac{d}{c-1}\right)^{n} - \frac{b}{a-1}.$$

The equation $f \circ g = g \circ h$ with $\deg(f) > 1$ (HT)

Theorem

Let $f, g, h \in \mathbb{C}[z]$ be non-constant polynomials such that $f \circ g = g \circ h$. Let $k = \gcd(\deg(f), \deg(g))$, $\deg(f) = kn$, $\deg(g) = km$. Then there are $s \in \mathbb{Z}_{\geq 0}$, $f_1, g_1, g_2, h_2, F, G, H \in \mathbb{C}[z]$ and linears $\ell_1, \ell_2 \in \mathbb{C}[z]$ such that

$$f = F \circ f_1, \; g = F \circ g_1 = g_2 \circ H, \; h = h_2 \circ H, \; f_1 \circ g_2 = g_1 \circ h_2$$

and one of the following options holds.

$$f_1 = T_n \circ \ell_1^{[-1]}, \; g_2 = \ell_1 \circ T_m, \; g_1 = T_m \circ \ell_2^{[-1]}, \; h_2 = \ell_2 \circ T_n.$$

$$f_1 = z^n \circ \ell_1^{[-1]}, \; g_2 = \ell_1 \circ z^s G(z^n), \; g_1 = z^s G(z)^n \circ \ell_2^{[-1]}, \; h_2 = \ell_2 \circ z^n.$$

$$f_1 = z^s G(z)^m \circ \ell_2^{[-1]}, \; g_2 = \ell_2 \circ z^m, \; g_1 = z^m \circ \ell_1^{[-1]}, \; h_2 = \ell_1 \circ z^s G(z^m).$$

Corollary

Let $f, h \in \mathbb{C}[z]$ *satisfy* $f \circ z^m = z^m \circ h$ *for some positive integer* m.

There is a polynomial $G \in \mathbb{C}[z]$ *such that* $f = G(z)^m$ *and* $h = G(z^m)$.

If $f = \sum_{j=0}^{n} a_j z^j$ *and* $h = b_n z^n + b_{n-r} z^{n-r} + O(z^{n-r-1})$ *with* $b_n \neq 0$, $b_{n-r} \neq 0$, $r > 0$, *then* $a_n = b_n^m$, $a_{n-1} = a_{n-2} = \ldots = a_{n-r+1} = 0$ *and* $a_{n-r} = m b_n^{m-1} b_{n-r}$. (If there is no such an r, then h is a monomial.)

Corollary

Let $f, h \in \mathbb{C}[z]$ *with* $\deg f = n$ *be such that* $f \circ T_m = T_m \circ h$ *for some positive integers* m, n *with* $\gcd(n, m) = k$, $n/k > 2, m/k > 2$.
Then there exists a $\delta \in \{-1, 1\}$ *such that*

$$f = \delta^m T_n, \quad h = \delta T_n.$$

The equation $f \circ g \circ h = h \circ g \circ f$

Theorem (HT, arXiv)

Suppose $f, g, h \in \mathbb{C}[z]$ *non-constant, not all linear, such that* $f \circ g \circ h = h \circ g \circ f$ *and* $\deg(f) \geq \deg(h)$. *Then one of the options holds:*

(i) *For linears* ℓ_1 *and* ℓ_2, $\ell_1^{[-1]} \circ f = h = f \circ \ell_2$, $g = \ell_2 \circ g \circ \ell_1$.

(ii) $g(z) = u_g z + v_g$, $h(z) = u_h z + v_h$ *either satisfy* $h = g^{[-1]}$, *or* $k, t \in \mathbb{Z}_{>1}$ *with* $t \mid k-1$, $u_g u_h$ *is a* t*-th root of unity and, for some* e_j*'s,*

$$f(z) = \sum_{j=0}^{(k-1)/t} e_j \left(z + \frac{u_g v_h + v_g}{u_g u_h - 1} \right)^{k-jt} - \frac{v_g u_h + v_h}{u_g u_h - 1}.$$

(iii) *There are linears* $\ell_1, \ell_2 \in \mathbb{C}[x]$ *and positive integers* α, β, γ *such that* $f = \ell_2^{[-1]} \circ T_\alpha \circ \ell_1$, $g = \ell_1^{[-1]} \circ T_\beta \circ \ell_2$, $h = \ell_2^{[-1]} \circ T_\gamma \circ \ell_1$.

(iv) *For linears* $\ell_1, \ell_2 \in \mathbb{C}[x]$, $\alpha, \beta, \gamma \in \mathbb{Z}_{>0}$, $c_g, c_h \in \mathbb{C}$, $c_g^{\gamma-\alpha} = c_h^{\alpha\beta-1}$,
$f = \ell_2^{[-1]} \circ z^\alpha \circ \ell_1$, $g = \ell_1^{[-1]} \circ c_g z^\beta \circ \ell_2$, $h = \ell_2^{[-1]} \circ c_h z^\gamma \circ \ell_1$.

(v) $G \in \mathbb{Z}$, *linear* ℓ, *roots of unity* ρ_j $(j = 1, 2)$ *and* $m > n$ *such that* $\hat{f} = \ell \circ f \circ \ell^{[-1]}$, $\hat{g} = \ell \circ g \circ \ell^{[-1]}$, $\hat{h} = \ell \circ h \circ \ell^{[-1]}$ *satisfy*
$\hat{g} \circ \hat{f} = \rho_1 G^{[m]}$, $\hat{f} = \hat{h} \circ \rho_2 G^{[m-n]}$, $G(\rho_j z) = \rho_j G(z)$ $(j = 1, 2)$.

Proof idea and variants

Let

$$f \circ g \circ h = h \circ g \circ f.$$

Then

$$f \circ g \circ h \ \circ g = h \circ g \circ f \circ g,$$

Hence, $F \circ H = H \circ F$ with $F = f \circ g$ and $H = h \circ g$.

For the four other non-trivial permutations:
$f \circ g \circ h = f \circ h \circ g$ can be treated by common f on the left.
$f \circ g \circ h = g \circ f \circ h$ implies $f \circ g = g \circ f$,
$f \circ (g \circ h) = (g \circ h) \circ f$
$(f \circ g) \circ h = h \circ (f \circ g)$.

The equation $f \circ g = h \circ g \circ f$

By degree comparison, we have $\deg(h) = 1$. Consider $f \circ g = \ell \circ g \circ f$.

Theorem (according to Schinzel's 2000 book, p. 51)

Let $f, g \in \mathbb{C}[z]$ The following two statements are equivalent.

1. *There exists a linear $\ell \in \mathbb{C}[z]$ such that*

$$f \circ g = \ell \circ g \circ f. \qquad (1)$$

2. *There exists a linear $\ell \in \mathbb{C}[z]$ such that either*

(a) $f = \ell \circ T_n \circ \ell^{[-1]}, \ g = \ell \circ T_m \circ \ell^{[-1]}$

or

(b) $f = \ell \circ az^n \circ \ell^{[-1]}, \ g = \ell \circ bz^m \circ \ell^{[-1]}$ *for some* $a, b \in \mathbb{C}$

or

(c) $f = \ell \circ G^{[n]} \circ \ell^{[-1]}, \ g = \ell \circ G^{[m]} \circ \ell^{[-1]}$ *for some* $G \in \mathbb{C}[z]$.

Proof by Ritt (1923), algebraic proof by Tortrat (1988).

Counterexample for Schinzel's statement

An example satisfying Schinzel's condition 1., but not his condition 2.:

$$f = 2z^3 + 6z^2 + 6z + 9,\ g = z^3 + 3z^2 + 3z + 4,\ \ell = \frac{1}{4}z + \frac{25}{4}.$$

Observe: $f = \ell_1 \circ g$.

More generally, let $f = h \circ g^{[r]}$
for some $r \in \mathbb{Z}_{>0}$ and some $f, g, h \in \mathbb{C}[z]$.
Then $f \circ g = \ell \circ g \circ f$ if and only if $h \circ g = \ell \circ g \circ h$.

Degree reduction

If $f = h \circ g$ for some $h \in \mathbb{C}[z]$, and

$$f \circ g = \ell \circ g \circ f,$$

then

$$h \circ g^{[2]} = f \circ g = \ell \circ g \circ f = \ell \circ g \circ h \circ g,$$

hence,

$$h \circ g = \ell \circ g \circ h.$$

If $\deg(f) = n, \deg(g) = m$, then $m \mid n$ and $\deg(h) = n/m$.
Reduction is possible if $\deg(g) \mid \deg(f)$ or $\deg(f) \mid \deg(g)$ in view of

$$g \circ f = \ell^{[-1]} \circ f \circ g.$$

This can be continued until $n = 1$ or $m = 1$ or ($m \nmid n$ and $n \nmid m$).

Degree induction

If $f \circ g = \ell \circ g \circ f$ and $h = f \circ g$, then

$$h \circ g = f \circ g^{[2]} = \ell \circ g \circ f \circ g = \ell \circ g \circ h.$$

This replaces (f, g) by $(f \circ g, g)$ with $\deg(h) = \deg(f) \times \deg(g)$.

Similarly, if $f \circ g = \ell \circ g \circ f$ and $h = g \circ f$, then $f \circ h = \ell \circ h \circ f$.
This replaces (f, g) by $(f, g \circ f)$ with $\deg(h) = \deg(f) \times \deg(g)$.

Start with (f_0, g_0, ℓ) with $f_0 \circ g_0 = \ell \circ g_0 \circ f_0$.
For $j = 0, 1, \ldots, s$, define either $f_{j+1} = f_j \circ g_j, g_{j+1} = g_j$ or $f_{j+1} = f_j, g_{j+1} = g_j \circ f_j$.
Then $f_j \circ g_j = \ell \circ g_j \circ f_j$ for all j.

Example. Suppose $f_0 \circ g_0 = \ell \circ g_0 \circ f_0$. Then $f \circ g = \ell \circ g \circ f$ for

$$f = f_0 \circ g_0^{[3]} \circ f_0 \circ g_0^{[2]}, \quad g = g_0 \circ f_0 \circ g_0^{[2]} \circ f_0 \circ g_0^{[3]} \circ f_0 \circ g_0^{[2]}.$$

Initial polynomials with $\deg(f_0) = 1$ or $\deg(g_0) = 1$

Let $\deg(g) = 1$. Set $g = \ell_1$. Then equation $f \circ \ell_1 = \ell \circ \ell_1 \circ f$.
This is a special case of equation $\ell_2 \circ f = f \circ \ell_1$.

Theorem

Let $\ell_2 = az + b$, $\ell_1 = cz + d$ and $\deg(f) = n > 1$.
Then $a = c^n$ and
A) if $c = 1$, then $(a, b, c, d) = (1, 0, 1, 0)$,
B) if $c \neq 1$, but c is a t-th root of unity, then

$$f = \sum_{j=0}^{(n-1)/t} e_j \left(z + \frac{d}{c-1}\right)^{n-jt} - \frac{b}{a-1},$$

C) If c is not a root of unity, then for some $e_0 \in \mathbb{C}$

$$f = e_0 \left(z + \frac{d}{c-1}\right)^{n} - \frac{b}{a-1}.$$

$\deg(f_0) \nmid \deg(g_0)$ and $\deg(g_0) \nmid \deg(f_0)$

In this case $f \circ g = \ell \circ g \circ f$ is of type $h \circ g = g \circ f$ with $h = \ell^{[-1]} \circ f$ and $\deg(f) > 1, \ \deg(g) > 1$.

Theorem

Let $k = \gcd(\deg(f), \deg(g))$, $\deg(f) = kn$, $\deg(g) = km$. Then there are $s \in \mathbb{Z}_{\geq 0}$, $h_1, g_1, g_2, f_2, F, G, H \in \mathbb{C}[z]$ and linears $\ell_1, \ell_2 \in \mathbb{C}[z]$ such that

$$h = H \circ f_1, \ g = H \circ g_1 = g_2 \circ F, \ f = f_2 \circ F, \ h_1 \circ g_2 = g_1 \circ f_2$$

and one of the following options holds.

$$h_1 = T_n \circ \ell_1^{[-1]}, \ g_2 = \ell_1 \circ T_m, \ g_1 = T_m \circ \ell_2^{[-1]}, \ f_2 = \ell_2 \circ T_n.$$

$$h_1 = z^n \circ \ell_1^{[-1]}, \ g_2 = \ell_1 \circ z^s G(z^n), \ g_1 = z^s G(z)^n \circ \ell_2^{[-1]}, \ f_2 = \ell_2 \circ z^n.$$

$$h_1 = z^s G(z)^m \circ \ell_2^{[-1]}, \ g_2 = \ell_2 \circ z^m, \ g_1 = z^m \circ \ell_1^{[-1]}, \ f_2 = \ell_1 \circ z^s G(z^m).$$

Final result

Theorem

Let $f, g, \ell \in \mathbb{C}[x]$, $k = \gcd(\deg(f), \deg(g))$, $\deg(f) = n$, $\deg(g) = m$.
Let ℓ **be a linear with** $\ell \neq z$ **and** $f \circ g = \ell \circ g \circ f$. *If* $m > 2k, n > 2k$, *then*

either *there are a linear* ℓ_2 *and* $\delta_1, \delta_2 \in \{-1, 1\}$ *such that*
$f = \ell_2 \circ \delta_1^{n/k} \delta_2^{n-1} T_n \circ \ell_2^{[-1]}, g = \ell_2 \circ \delta_1^{m/k} \delta_2^{m} T_m \circ \ell_2^{[-1]}$,
$\ell = \ell_2 \circ \delta_1^{(n-m)/k} \delta_2^{n-1} \circ \ell_2^{[-1]}$,

or

$f = \ell_2 \circ az^n \circ \ell_2^{[-1]},\ g = \ell_2 \circ bz^m \circ \ell_2^{[-1]}, \ell = \ell_2 \circ a^{1-m} b^{n-1} z \circ \ell_2^{[-1]}$ *for some* $(a, b \in \mathbb{C})$,

or

$f = f_s, g = g_s$ *for some positive integer s such that* f_0 *or* g_0 *is linear,* $f_0 \circ g_0 = \ell \circ g_0 \circ f_0$ *and*

$$f_j = f_{j-1} \circ g_{j-1}, g_j = g_{j-1} \ \text{ or } \ f_j = f_{j-1}, g_j = g_{j-1} \circ f_{j-1} \ \ (j = 1, 2, \ldots, s).$$

Tortrat's Proposition 11.

Theorem (Proposition 8)

Let $f, g \in \mathbb{C}[z]$ be of degree ≥ 2.
If $f \circ g = g \circ f$, then $\mathcal{P}_f = \mathcal{P}_g$.
If $\mathcal{P}_f = \mathcal{P}_g$, then there is a linear ℓ such that $f \circ g = \ell \circ g \circ f$.

Theorem (Proposition 11)

1. *There exists a linear $\ell \in \mathbb{C}[z]$ such that $f \circ g = \ell \circ g \circ f$.*

$f, g \in \mathbb{C}[z]$ of degree ≥ 2 are such that $\mathcal{P}_f = \mathcal{P}_g$ if and only if
there exists a linear $\ell \in \mathbb{C}[z]$ such that either
(a) $f = \ell \circ T_n \circ \ell^{[-1]}, \; g = \ell \circ T_m \circ \ell^{[-1]}$
or
(b) $f = \ell \circ az^n \circ \ell^{[-1]}, \; g = \ell \circ bz^m \circ \ell^{[-1]}$ *for some $a, b \in \mathbb{C}$*
or, for some $\ell_1, \ell_2, G \in \mathbb{C}[z]$, ℓ_1, ℓ_2 linear,
(c) $f = \ell_1 \circ G^{[n]} \circ \ell^{[-1]}, \; g = \ell_2 \circ G^{[m]} \circ \ell^{[-1]}$.