ON THE COMPOSITION OF A PRIME TRANSCENDENTAL FUNCTION AND A PRIME POLYNOMIAL

TUEN-WAI NG AND CHUNG-CHUN YANG
ON THE COMPOSITION OF A PRIME TRANSCENDENTAL FUNCTION AND A PRIME POLYNOMIAL

Tuen-Wai Ng and Chung-Chun Yang

Let \( f, g \) be transcendental entire functions and \( p, q \) be nonlinear polynomials with \( \deg p \neq 3, 6 \). Suppose that \( f \) and \( p \) are prime and \( f(p(z)) = g(q(z)) \), then \( f = g \circ L \) and \( p = L^{-1} \circ q \), where \( L \) is a linear polynomial. Similar results for \( p(f(z)) = q(g(z)) \) are also obtained.

1. Introduction and Main Results.

A meromorphic function \( F(z) \) is said to has a factorization with left factor \( f \) and right factor \( g \) provided

\[ F(z) = f(g(z)), \]

where \( f \) is meromorphic and \( g \) is entire (\( g \) may be meromorphic when \( f \) is rational). A nonlinear meromorphic function \( F(z) \) is called prime (pseudo-prime) if every factorization of form (1) implies that either \( f \) is bilinear or \( g \) is linear (either \( f \) is rational or \( g \) is a polynomial). Clearly, a prime function is an analogy of a prime number. Over the past thirty years, many classes of prime or pseudo-prime functions have been obtained (see [2]).

As an analogue of the unique factorizability of natural numbers, one can also define that concept for entire functions. Suppose an entire function \( F \) has two factorizations \( f_1 \circ f_2 \circ \cdots \circ f_m(z) \) and \( g_1 \circ g_2 \circ \cdots \circ g_n(z) \) into nonlinear entire factors. If \( m = n \) and if there exist linear polynomials \( L_j \) (\( j = 1, 2, 3, \ldots, n-1 \)) such that the relations

\[ f_1(z) = g_1 \circ L_1^{-1}, \quad f_2(z) = L_1 \circ g_2 \circ L_2^{-1}, \quad \ldots, \quad f_n(z) = L_{n-1} \circ g_n(z) \]

hold simultaneously, then the two factorizations are called equivalent. If any two factorizations of \( F(z) \) into nonlinear, prime entire factors are equivalent to each other, then \( F \) is called uniquely factorizable in entire sense.

As far as just polynomial factors are concerned, it is easy to exhibit functions which are not uniquely factorizable in entire sense, for instance, \( z^3 \circ z^2 = z^2 \circ z^3 \).

Therefore, the following question is not without interest.
Problem (A). Suppose $f$ and $g$ are prime entire functions and one of them is transcendental, will $F(z) = f \circ g(z)$ be uniquely factorizable in entire sense?

Counter-example. Take $f(z) = z^2, g(z) = z e^{z^2}, f_1(z) = z e^{2z}$ and $g_1(z) = z^2$. All of them are prime functions (see [2]) and $f \circ g = f_1 \circ g_1$ are two nonequivalent factorizations of $z^2 e^{z^2}$.

In this paper, we shall consider the following problems. Let $f$ and $p$ be two prime entire functions where $f$ is transcendental and $p$ is a polynomial. Suppose that $f \circ p = g \circ q$ or $p \circ f = q \circ g$. Under what conditions on the entire functions $g, q$ will these factorizations be equivalent?

From the above counterexample, it is clear that two factorizations of a function $F = h \circ k = h_1 \circ k_1$ may not be equivalent. Therefore, we need to have some further assumptions on these factors $h, h_1, k$ and $k_1$.

With this in mind, we have come up with the following results. The functions $f, g, p$ and $q$ considered below are all entire and nonlinear.

Theorem 1. Let $f, p$ be two non-periodic prime entire functions and $p$ be a polynomial. Suppose that $p \circ f = q \circ g$ and both $f, g$ are transcendental. Then $p = q \circ L^{-1}$ and $f = L \circ g$, where $L$ is a linear polynomial.

Theorem 2. Let $f, p$ be two prime entire functions and $f$ be transcendental. Suppose that $p \circ f = q \circ g$ and both $p, q$ are polynomials. Then $p = q \circ L^{-1}$ and $f = L \circ g$, where $L$ is a linear polynomial.

Theorem 3. Let $f, p$ be two prime entire functions and $f$ be transcendental. Suppose that $f \circ p = g \circ q$ and both $p, q$ are polynomials with $\deg p \neq 3, 6$. Then $f = g \circ L$ and $p = L^{-1} \circ q$, where $L$ is a linear polynomial.

Theorem 1, 2 and 3 deal with the relationships between polynomials $p$ and $q$, transcendental functions $f$ and $g$ when we have factorizations of the form $p \circ f = q \circ g$ or $f \circ p = q \circ g$. It is natural to investigate the case $f \circ p = q \circ g$.

Theorem 4. Let $f$ and $g$ be two transcendental entire functions, $p$ and $q$ be two nonlinear polynomials with degree $n$ and $m$ respectively. If $f \circ p = q \circ g$ and $p$ is not a right factor of $g$, then $\deg p \leq \deg q$. In particular, the conclusion is true when $g$ is prime.

Remark 1. Let $f(z) = e^z, g(z) = e^{z^3}, p(z) = z^3$ and $q(z) = z^2$. Then $f \circ p = q \circ g$ and $\deg p > \deg q$. Therefore, the condition that $p$ is not a right factor of $g$ is essential.

Definition 1. Let $F(z)$ be an nonconstant entire function. An entire function $g(z)$ is a generalized right factor of $F$ (denoted by $g \leq F$) if there exists a function $f$, which is analytic on the image of $g$, such that $F = f \circ g$. If such $f$ is entire, $g$ will be a right factor of $F$ (denoted by $g|F$).
Definition 2. If \( h \leq f \) and \( h \leq g \), we say that \( h \) is a generalized common right factor of \( f \) and \( g \). If \( g \leq F \) and \( f \leq F \), we say that \( F \) is a generalized common left multiple of \( f \) and \( g \).

The existence and uniqueness problems of the greatest generalized common right factor and the least generalized common left multiple for a given pair of entire functions were solved by A. Eremenko and L.A. Rubel as follows.

Lemma 1 ([4]). Any pair of non-constant entire functions has (up to a linear factor) a unique greatest generalized common right factor \( h \), greatest in the sense that any generalized common right factor of \( f \) and \( g \) is a generalized right factor of \( h \).

Lemma 2 ([4]). Suppose that \( f \) and \( g \) have a generalized common left multiple. Then \( f \) and \( g \) have (up to a linear factor) a unique least generalized common left multiple \( F \), least in the sense that \( F \) is a generalized right factor of any generalized common left multiple of \( f \) and \( g \).

The proof of Theorem 1 is mainly based on the following lemma.

Lemma 3 ([10]). Let \( f \) and \( g \) be two entire functions. Suppose that there exist two nonconstant complex functions \( k \) and \( R \) such that \( F = R \circ f = k \circ g \) is meromorphic. If \( g \) is transcendental and \( R \) is rational, then there exists a transcendental entire function \( h \) satisfying \( h \leq f \) and \( h \leq g \).

Proof of Theorem 1. By Lemma 3, there exists a transcendental entire function \( h \) satisfying \( h \leq f \) and \( h \leq g \). Hence, \( f = h_1 \circ h \) and \( g = h_2 \circ h \), where \( h_1, h_2 \) are analytic on the image of \( h \). If the image of \( h \) is \( \mathbb{C} \setminus \{a\} \), then \( h = a + e^k \) for some entire function \( k \). Without loss of generality, we may assume \( a = 0 \) so that \( f(z) = h_1(e^w) \circ k(z) \). The primeness of \( f \) will force \( k \) to be linear. This contradicts the assumption that \( f \) is not a periodic function. So the image of \( h \) must be the whole plane. This implies that both \( h_1, h_2 \) are entire and \( p \circ h_1 = q \circ h_2 \) on \( \mathbb{C} \). Since \( f = h_1 \circ h \) is prime, \( h_1 \) must be linear. From \( p \circ h_1 = q \circ h_2 \), \( h_2 \) must also be linear as \( p \) is prime. Take \( L = h_1 \circ h_2^{-1} \) and we are done. \( \square \)

The proof of Theorem 2 is similar, we simply apply Lemma 4 below instead of Lemma 3.

Lemma 4 ([6]). Let \( f \) and \( g \) be two entire functions. Suppose that there exist two nonconstant polynomials \( p \) and \( q \) such that \( p \circ f(z) = q \circ g(z) \). Then there exist an entire function \( h \) and rational functions \( U(z) \) and \( V(z) \) such that

\[
    f(z) = U \circ h(z), \quad g(z) = V \circ h(z).
\]

To prove Theorem 4, we need the following lemma which can be used to prove Lemma 3.
Lemma 5 ([10]). Let $f$ and $g$ be two entire functions. Suppose that there exist two nonconstant functions $h_1$ and $h_2$ so that $F = h_1(f(z)) = h_2(g(z))$ and $F$ is meromorphic. Suppose further that there exist $k \geq 2$ distinct points $z_1, \ldots, z_k$ such that $F'(z_i) \neq 0, \infty$ for all $i$ and
\[
\begin{cases}
  f(z_1) = f(z_2) = \ldots f(z_k) \\
  g(z_1) = g(z_2) = \ldots g(z_k).
\end{cases}
\]

Then, there exists an entire function $h(z)$ (independent of $k$ and $z_i$'s) with $h \leq f$, $h \leq g$ and $h(z_1) = h(z_2)$ for all $2 \leq i \leq k$.

Proof of Theorem 4. By Lemma 1, there exists a generalized greatest common right factor $k$ of $p$ and $g$. Since, $p$ is a polynomial, $k$ is actually the greatest common right factor of $p$ and $g$. Let $p_1$ and $g_1$ be entire functions such that $p = p_1 \circ k$ and $g = g_1 \circ k$. Hence, $f \circ p_1 = q \circ g_1$ on $C$ and $p_1, g_1$ do not have any nonlinear common right factor. $p_1$ is nonlinear as $p$ is not a right factor of $g$. If we can show that $\deg p_1 \leq \deg g_1$, then $\deg p \leq \deg g$. Therefore, we may assume that $p$ and $g$ do not have any nonlinear common right factor. Suppose that $n > m$. Define $E = \{p(z)|F'(z) = 0\}$, where $F = f \circ p$. Then $E$ is a countable set. Therefore, we can choose $A \in C - E$ so that the equation $p(z) = A$ has $n \geq 2$ distinct roots $z_1, \ldots, z_n$. Since $f(A) = f(p(z_i)) = q(g(z_i))$, $g(z_i)$ are roots of the equation $q(z) = f(A)$ which has at most $m$ roots. $n > m$ implies that there exist two distinct pairs $z_i, z_j$ such that $g(z_i) = g(z_j)$. Note that $p(z_i) = p(z_j) = A$ and $F'(z_i), F'(z_j) \neq 0$. By Lemma 5, there exists an entire function $h$ with $h \leq p$, $h \leq g$ and $h(z_i) = h(z_j)$. Clearly $h$ is a polynomial. Hence, there exists a nonlinear $h$ such that $h|p$ and $h|g$. This is impossible and we must have $n \leq m$.

In Theorem 3, we only assume that $p$ and $q$ are polynomials. If we further restrict $p$ and $q$ to have $\deg p = \deg q \geq 3$, then the conclusion of Theorem 3 can be drawn directly from the following lemma.

Lemma 6 ([5]). Let $p$ and $q$ be two polynomials with the same degree. Suppose there exist entire functions $f$ and $g$ such that $f \circ p = g \circ q$. Then one of the following two cases holds:

(a) $p(z) = L \circ q(z)$ where $L$ is a linear polynomial.
(b) $p(z) = (r(z))^2 + a$ and $q = b(r(z) + c)^2 + d$, where $a, b, c, d$ are complex numbers.

The above type of results were first investigated by I.N. Baker and F. Gross in [1] and then L. Flatto in [5]. Finally, S.A. Lysenko in [8] gives an algebraic necessary and sufficient condition for the existence of meromorphic $f$ and $g$ satisfy $f \circ p = g \circ q$.

The proof of Theorem 3 is based on a method developed by S.A. Lysenko in [8] which depends on a fundamental result of local holomorphic dynamics.
2. Local holomorphic dynamics.

Let $X$ be a Riemann surface and let $f : (X, a) \to (X, a)$ denote a mapping defined in some neighbourhood of a point $a$ on $X$ with $f(a) = a$. A germ of a mapping $f : (X, a) \to (X, a)$ is defined to be the equivalent class of all mappings which coincide with $f$ in some neighbourhood of $a$ and it is denoted by $[f]$. We say that $f$ is conformal at $a$ if $f$ is analytic in some neighbourhood of $a$ and $f'(a) \neq 0$. In this case $f$ will have an inverse $f^{-1}$ in a neighbourhood of $a$. Let $\Gamma(X, a)$ be the set of all germs of conformal mapping $(X, a) \to (X, a)$. We define $[f] \circ [g]$ by $[f \circ g]$. Note that if $[f] = [f_1]$, then $f \equiv f_1$ on any region for which both $f$ and $f_1$ are analytic. Hence, the binary operation $\circ$ is well-defined. Clearly, the inverse of $[f]$ under $\circ$ is $[f^{-1}]$.

Therefore, $(\Gamma(X, a), \circ)$ is a group. Note that two germs in $(\Gamma(X, a), \circ)$ are the same if they have the same Taylor series expansions about $a$. Therefore, from time to time, we shall simply denote the germ $[f]$ by its Taylor series.

For example, elements of $\Gamma(\mathbb{CP}^1, \infty)$ are of the form $a_1 z + a_0 + \frac{a_{-1}}{z} + \frac{a_{-2}}{z^2} + \cdots$ with $a_1 \neq 0$. While elements of $\Gamma(\mathbb{C}, 0)$ are of the form $a_1 z + a_2 z^2 + a_3 z^3 + \cdots$ with $a_1 \neq 0$.

We simply denote $\Gamma(\mathbb{CP}^1, \infty)$ by $\Gamma$.

**Definition 3.** Let $p$ be a nonconstant polynomial. Since $p^{-1}(\{\infty\}) = \{\infty\}$, we can define a group $T_p = \{g \in \Gamma \mid p \circ g = p\}$. Then, it can be shown that $T_p$ is a cyclic subgroup of $\Gamma$ and its order equals to $\deg p$.

**Example 1.** $T_z^n = \{\lambda z \mid \lambda^n = 1\}$ and $T_{(z+1)^m} = \{\delta z + \delta - 1 \mid \delta^m = 1\}$.

$T_p$ is so-called a discrete invariant subgroup of $\Gamma$. In fact, we have the following definition.

**Definition 4.** A subgroup $G$ of $\Gamma$ is discrete invariant if there exists a non-constant function $F$, meromorphic in a punctured neighbourhood of infinity in $\mathbb{C}$, such that $F(g(z)) = F(z)$ for all $g \in G$.

In [11], A.A. Shcherbakov proved that if $G \subset \Gamma$ is discrete invariant, then $G$ is a solvable group.

We also need another important necessary condition for $G \subset \Gamma$ to be discrete. Define $\Gamma_1 = \left\{ g \in \Gamma \mid g = z + a_0 + \frac{a_{-1}}{z} + \frac{a_{-2}}{z^2} + \cdots \right\}$ and $\Gamma_0 = \left\{ g \in \Gamma \mid g = z + \frac{a_{-1}}{z} + \frac{a_{-2}}{z^2} + \cdots \right\}$. Clearly, $\Gamma_1/\Gamma_0$ is isomorphic to $(\mathbb{C}, +)$.

**Lemma 7 ([8]).** Let $G \subset \Gamma$, $G_1 = G \cap \Gamma_1$ and $G_0 = G \cap \Gamma_0$. If $G$ is discrete invariant, then $G_1/G_0$ is isomorphic to a discrete subgroup of $(\mathbb{C}, +)$.

**Example 2.** Let $f, g$ be nonconstant meromorphic functions and $p, q$ be nonconstant polynomials. Suppose that $F(z) = f(p(z)) = g(q(z))$, then the group generated by $T_p$ and $T_q$, denoted by $[T_p, T_q]$, is a discrete invariant.
subgroup of $\Gamma$. Hence, $[T_p, T_q]$ is solvable. If we take $p(z) = z^n$, $q(z) = (z + 1)^m$ and $G = [T^n, T_{(z+1)^m}]$, then $G_1 \subset \{T_b(z) = z + b \mid b \in \mathbb{C}\}$ and $G_0 = \{z\}$. Now $G_1 \cong G_1/G_0$ which is isomorphic to a discrete subgroup of $(\mathbb{C}, +)$.

$T_p$ and $[T_p, T_q]$ are the main objects we shall study. The following two lemmas which were proved by using Galois Theory will be needed in the proof of Theorem 3.

**Lemma 8** ([8]). Let $p$ and $q$ be two nonconstant polynomials. Define $H_{p,q} = \{ \sigma \in T_p \mid \rho \sigma = \sigma \rho \text{ for all } \rho \in T_q \}$. Then $H_{p,q} = T_{p_1}$, where $p_1$ is a right factor of $p$.

**Lemma 9** ([8]). If $[T_p, T_q]$ is finite, then there exist two nonconstant rational functions $R_1, R_2$ such that $R_1 \circ p(z) = R_2 \circ q(z)$.

If $[T_p, T_q]$ is infinite, then $[T_p, T_q]$ must be non-Abelian as both $T_p$ and $T_q$ are cyclic. Moreover, if $[T_p, T_q]$ is also solvable, then we can construct some groups that are isomorphic to $[T_p, T_q]$. These groups come from local holomorphic dynamics and are easier to deal with.

**Definition 5.** Let $w$ be a holomorphic vector field on $V \subset \mathbb{C}$. Associated with $w$, it is well known that there exists a unique local phase flow $g_w : U \times V \to \mathbb{C}$ which is a solution of the Cauchy problem

$$
\frac{d}{dt} g_w(t, z) = w(g_w(t, z)), \quad g_w(0, z) = z,
$$

where $U \subset \mathbb{R}$ is a sufficiently small neighbourhood of 0. For brevity, we denote $g_w(t, z)$ by $g_w^t(z)$ the time-$t$ transformation for the flow of the holomorphic vector field $w$. Moreover, we have the following important property:

$$
g_w^{t+s}(z) = g_w^t(g_w^s(z)),
$$

in the sense that if one side of (4) is defined, so is the other, and they are equal. If we extend the definition of $g_w^t(z)$ for all $t \in \mathbb{C}$, then $g_w^t(z)$ (possibly divergent) will be a formal solution of Equation (3), which will be denoted as $\hat{g}_w^t(z)$.

**Definition 6.** If $f : V \to W$ is a bijective conformal mapping, then the forward image $f_*w$ of the vector field $w$ on $V$ is defined as

$$(f_*w)(z) = f'(f^{-1}(z)) \times w(f^{-1}(z)),$$

for all $z \in W$.

Let $k$ be a natural number. We denote by $g_{z_{k+1}}$ the time-$t$ transformation for the flow of the holomorphic vector field $z^{k+1}\frac{\partial}{\partial z}$. Express $g_{z_{k+1}}^t$ as $a_0(t) + a_1(t)z + a_2(t)z^2 + \cdots$ and substitute it into Equation (3). Comparing the coefficient of the constant term, we have $a_0'(t) = a_0^{k+1}(t), \quad a_0(0) = 0.$
Hence, \( a_0(t) \equiv 0 \) on some neighbourhood of zero. By repeating this process, it is easy to check that \( g_{z,k+1}^t(z) = z + tz^{k+1} + \cdots \). Therefore, for each sufficiently small real \( t \), \( g_{z,k+1}^t(z) \) is conformal in some neighbourhood of zero with \( g_{z,k+1}^t(0) = 0 \). Note that for complex number \(|t| < 1\), we have \( g_{z}^t(z) = z + tz^2 + t^2 z^3 + t^3 z^4 + \cdots \) is conformal in some neighbourhood of zero.

Now, we consider the set of germs

\[
G(k) = \{ \lambda g_{z,k+1}^t : (\mathbb{C},0) \to (\mathbb{C},0) \mid \lambda \in \mathbb{C}^* = \mathbb{C} - \{0\}, t \in \mathbb{C} \}.
\]

We shall show that \( G(k) \) under composition is a group. For brevity, denote \( \lambda g_{z,k+1}^t \) by \((\lambda,t)\). For any \( \mu \in \mathbb{C}^* \), let \( \mu(z) = \mu z \), it is easy to check that \( \mu^{-1} \circ g_{z,w}^t \circ \mu \) satisfies condition (3) and hence \( g_{\mu z,w}^t \circ \mu = \mu \circ g_{z,w}^t \). Similarly, we have \( g_{z,k+1}^t = g_{\mu z,k+1}^{\mu^{-1} t} \). Now,

\[
(5) \quad g_{z,k+1}^t \circ \mu = g_{\mu z,k+1}^{\mu^{-1} t} \circ \mu = \mu \circ g_{z,k+1}^t.
\]

(4) and (5) imply that \( G(k) \) is a group under composition. From (4) and (5), the multiplication table for \( G(k) \) has the following form:

\(
(\lambda,t) \times (\mu,s) = (\lambda \mu, t \mu^{-k} + s).
\)

With the above formula, it is easy to prove that the subgroup \( C(k) = \{ \lambda z = \lambda g_{z,k+1}^0 \in G(k) \mid \lambda^k = 1 \} \) is the center of \( G(k) \) (i.e., set of element commutes with all elements of \( G(k) \)).

**Definition 7.** Let \( G \) and \( G_1 \) be two groups of germs of conformal mappings \((\mathbb{C},0) \to (\mathbb{C},0)\). \( G \) and \( G_1 \) is said to be formally equivalent if there exists an isomorphism \( K : G \to G_1 \) and a formal series \( \hat{h} \) whose constant term is zero and the linear term is nonzero, such that for any \( f \in G \),

\[
\hat{h}^{-1} \circ f \circ \hat{h} = K f.
\]

The hat over a symbol stands for the corresponding formal series.

Now, we can state the main lemma as follows.

**Lemma 10 ([3]).** A finitely generated non-Abelian solvable group of all germs of conformal mapping \((\mathbb{C},0) \to (\mathbb{C},0)\) is formally equivalent to a finitely generated subgroup of \( G(k) \) for some \( k \).

**Remark 2.** Let \( J(z) = 1/z \) and \( G \) be a subgroup of \( \Gamma(\mathbb{C}P^1, \infty) \). Then \( J^{-1}GJ = \{ J^{-1} \circ g \circ J \mid g \in G \} \) is a subgroup of \( \Gamma(\mathbb{C},0) \). Clearly \( G \) and \( J^{-1}GJ \) are isomorphic and from now on, we shall identify \( G \) with \( J^{-1}GJ \) frequently. For example, \( T_m^\infty \) is identified with \( J^{-1}T_m^\infty J = \{ \lambda z \mid \lambda^m = 1 \} = \{ \lambda g_{z,0}^0 \mid \lambda^m = 1 \} \) and \( T_{n+1}m^\infty \) is identified with \( J^{-1}T_{n+1}m^\infty J = \{ \delta z + \delta(\delta - 1)z^2 + \delta(\delta - 1)^2 z^3 + \cdots \mid \delta^m = 1 \} = \{ \delta g_{z,0}^0 \mid \delta^m = 1 \} \).
3. Proof of Theorem 3.

Let \( F(z) = f(p(z)) = g(q(z)) \). From Example 2, we know that \([T_p, T_q]\) is solvable. We shall consider two cases: i) \([T_p, T_q]\) is finite and ii) \([T_p, T_q]\) is infinite.

Suppose that \([T_p, T_q]\) is finite, then by Lemma 9, there exist two nonconstant rational functions \( R_1, R_2 \) such that \( R_1 \circ p(z) = R_2 \circ q(z) \). Express \( R_i \) as \( \frac{P_i}{Q_i} \), where \( P_i \) and \( Q_i \) are polynomials and do not have any common zero. Without loss of generality, we may assume that \( P_1 \) is nonconstant. Since \( P_i \) and \( Q_i \) do not have any common zero, we have \( F_1 = P_1(p(z)) = A P_2(q(z)) \) for some nonzero constant \( A \). By Lemma 2, there exists a nonconstant entire function \( F_2 \), which is the least generalized common left multiple of \( p \) and \( q \), such that \( F_2 \leq F_1 \) and \( F_2 \leq F \). From \( F_2 \leq F_1 \), it follows that \( F_2 \) is a polynomial and hence \( F_2 | F_1 \) and \( F_2 | F \). Now, we can let \( F_2 = h \circ p = k \circ q \) for some polynomials \( h, k \). Note that \( F_2 | F \) which implies \( h | f \). Since \( f \) is prime and transcendental, \( h \) must be linear. Therefore, \( p = h^{-1} \circ k \circ q \), where \( h^{-1} \circ k \) is linear because \( p \) is prime and \( q \) is nonlinear. So, we are done for case i).

If \([T_p, T_q]\) is infinite, then it is not-Abelian as both \( T_p, T_q \) are finite order cyclic groups. Since \([T_p, T_q]\) is also solvable, it follows from Lemma 10 that \([T_p, T_q]\) is formally equivalent to a subgroup of \( G(k) \) for some natural number \( k \). Let \( d = \text{lcm}(n, m) \) where \( n = \text{deg} p \) and \( m = \text{deg} q \). Let \( \lambda g^t_{s} = \mu g^t_{r} \) be the generators of \( T_p \) and \( T_q \) respectively. From the multiplication table of \( G(k) \), \( \lambda^n = 1 \) and \( \mu^m = 1 \). Hence, all elements of \([T_p, T_q]\) are in \( G_d(k) = \{ \lambda g^t_{s} \in G(k) | \lambda^d = 1 \} \). Therefore, \([T_p, T_q]\) is actually formally equivalent to a subgroup of \( G_d(k) \).

By Lemma 8 and the fact that \( p \) is prime, \( H_{p,q} = T_p \) or \( T_{id} \). If \( H_{p,q} = T_p \), then \([T_p, T_q]\) must be abelian which is impossible. So, we have \( H_{p,q} = T_{id} = \{z\} \). It is easy to check that if \( h \in G_k(k) \) is an element of finite order, then \( h \in C(k) \). Hence, \( T_p \cap G_k(k) \subset C(k) \). Note that \( C(k) \) is the center of \( G(k) \) and so \( T_p \cap G_k(k) \subset H_{p,q} = \{z\} \). Now, we claim that \( g = \gcd(n, k) = 1 \). Let \( (\lambda, t) \) be a generator of \( T_p \). Then, it is very easy to check that \( (\lambda, t)^\frac{n}{g} \) is an element of \( T_p \cap G_k(k) \). Therefore, \( (\lambda, t)^\frac{n}{g} = (1, 0) \) and hence \( \frac{n}{g} = n \). We get \( g = \gcd(n, k) = 1 \).

We first consider the case that \( q \) is prime. Then, we also have \( \gcd(m, k) = 1 \). So, if \( d = \text{lcm}(n, m) \), then \( \gcd(d, k) = 1 \). We define a map \( f : G_d(k) \to G_d(1) \) by \( f(\lambda g^t_{s}) = \lambda^g g^t_{s} \). Clearly, \( f \) is a group homomorphism and surjective. The condition that \( \gcd(d, k) = 1 \) implies that \( f \) is also injective. Therefore \([T_p, T_q]\) is isomorphic to a subgroup of \( G_d(1) \).
Let \( \lambda g_{z_2}^2 \) and \( \delta g_{z_2}^2 \) be the elements of \( G_d(1) \) corresponding to generators of \( T_p \) and \( T_q \) respectively. Note that
\[
(1, 0) = \text{id} = \lambda g_{z_2}^2 \circ \lambda g_{z_2}^2 \circ \cdots \circ \lambda g_{z_2}^2 (n \text{ times}) = (\lambda^n, t(\lambda^{-(n-1)} + \cdots + \lambda^{-1} + 1)).
\]
So, \( \lambda \) (respectively \( \delta \)) is a primitive \( n \)th root of unity (respectively a primitive \( m \)th root of unity).

By choosing a suitable number \( r \), we have \((1, r) \times (\lambda, t) \times (1, -r) = (\lambda, 0)\). Therefore, with this conjugation, we may assume \( t = 0 \) and this implies that \( s \neq 0 \), for otherwise \([T_p, T_q]\) will be abelian. By using the automorphism \( \lambda g_{z_2}^2 \rightarrow \lambda g_{z_2}^d (c \neq 0) \) of \( G_d(1) \), we may also assume that \( s = \delta - 1 \).

Hence the generators are of the form \( \delta g_{z_2}^0 \) and \( \delta g_{z_2}^{\delta - 1} \). From Remark 2, we know that they generate \( T_{zn} \) and \( T_{(z+1)m} \) respectively. Therefore \([T_p, T_q]\) is isomorphic to \( G = [T_{zn}, T_{(z+1)m}] \). From Example 2, \( G_1 \cong (G_1/G_0) \cong ([T_p, T_q] \cap \Gamma_1)/([T_p, T_q] \cap \Gamma_0) \) which is isomorphic to a discrete subgroup of \((\mathbb{C}, +)\) by Lemma 7.

Suppose \( T_b \in G_1 \), then \( T_{\delta b} \) is also in \( G_1 \). It is because \( z + \delta b = (\delta z + \delta - 1) \circ (z + b) \circ (\delta^{-1} z + \delta^{-1} - 1) \). Similarly, \( T_{\delta b} \in G_1 \) and hence \( T_{\delta b} \in G_1 \), where \( \epsilon \) is a \( d \) th root of unity with \( d = \text{lcm} (n, m) \). Since \( G_1 \) is isomorphic to a nontrivial discrete subgroup of \((\mathbb{C}, +)\), it is easy to show that either \( G_1 = \{ T_{na} \mid n \in \mathbb{Z} \} \) or \( G_1 = \{ T_{nb + mc} \mid n, m \in \mathbb{Z} \} \) for some \( a, b, c \in \mathbb{C} \) and \( b/c \) being irrational (see [9], p. 63). We consider the first case: \( T_a \in G_1 \), which implies \( T_{2z a + a} \in G_1 \). Hence, \( T_{2a \cos \frac{2\pi}{d}} = T_{e^{-i \times (2^a + a)} } \in G_1 \). Thus, \( 2 \cos \frac{2\pi}{d} \) is some integer which can only be 0, \( \pm 1 \) or \( \pm 2 \). So, it follows that \( d \in \{2, 3, 4, 6\} \). With similar argument, we can have the same conclusion for the second case.

If \( n = m = 3, 4, 6 \), then it follows from Lemma 6 that \( p = L \circ q \), where \( L \) is linear. Hence, \([T_p, T_q] = T_p\) is finite, which is a contradiction.

If \( n = m = 2 \), without loss of generality we may assume that \( p(z) = z^2 \) and \( q(z) = (z + c)^2 \). Then we have \( F_1 = \cos \sqrt{z} \circ p = \cos (\sqrt{z} - c) \circ q \). By Lemma 2, there exists a nonconstant entire function \( F_2 \), which is the least generalized common left multiple of \( p \) and \( q \), such that \( F_2 \leq F_1 \) and \( F_2 \leq F \).

Let \( F_2 = h \circ p = k \circ q \), it follows that \( h \leq f \) and \( h \leq \cos \sqrt{z} \). Thus \( h \) is not periodic. By similar argument used in the proof of Theorem 1, we have \( h \mid f \). Since \( f \) is prime, \( h \) is linear or \( h = L \circ f \) for some linear function \( L \). \( h \) is linear implies \( p = h^{-1} \circ k \circ q \) which is impossible again. Therefore, \( h = L \circ f \).

Hence, \( \cos \sqrt{z} \) has a prime transcendental right factor \( f \). Write \( \cos \sqrt{z} \) as \( h_1 \circ f \). Thus \( \cos z = h_1 \circ f(z^2) \). From Theorem 3.10 in [2], \( f(z^2) = \cos \frac{z}{m} \) which implies \( f(z) = \cos \frac{\sqrt{z}}{m} \). This is impossible as \( \cos \frac{\sqrt{z}}{m} \) is not a prime function.

Now, we can assume that \( n \neq m \) and hence \( d \neq 2, 3, 4 \). \( d = 4 \) implies that one of \( n, m \) equals to 2. We may assume without loss of generality that \( n = 2 \) and \( p = z^2 \), \( q(z) = z^4 + a_3 z^3 + a_2 z^2 + a_1 z \). Since \( f(p(z)) = f(p(-z)) \),
$g(q(z)) = g(q(-z))$, and because $q$ is prime, Lemma 6 implies that $q(z) = L \circ q(-z)$. Note that $L$ is linear, then $a_3 = a_1 = 0$ and hence $q$ is not prime which is impossible. If $d = 6$, $n$ can only be 2,3 or 6. The case for $n = 2$ can be treated similar as above and the case $n = 3, 6$ are excluded from our considerations.

For general $q$, we can express $q$ as $q_2 \circ q_1$ where $q_1$ is prime. From the above discussion, we have $f = g \circ q_2 \circ L^{-1}$ and $p = L \circ q_1$. Thus, $f$ is prime implies that $q_2$ is linear and we are done.

4. Further discussions.

In Theorem 3, we assume that both the right factors $p, q$ have polynomial growth. We can also restrict the left factors $f, g$ to have comparable growth rate and ask the following question.

Problem (B). Let $f$ and $p$ be two prime entire functions and $p$ is a polynomial. Suppose that $F = f \circ p = g \circ q$ and both $f, g$ are transcendental. Are the two factorizations of $F$ equivalent?

This problem is closely related to Problem C below (proposed by C.C. Yang, see e.g., [7], p. 124), which remains unsolved for more than a decade.

Problem (C). Let $f$ be a pseudo-prime transcendental meromorphic function and $p$ be a polynomial of degree $\geq 2$. Must $f(p(z))$ be pseudo-prime?

If the answer to Problem C is positive, then the function $q$ in Problem B must be a polynomial and this reduces to the case handled in Theorem 3. One may try to solve Problem C for the special case that $p(z) = z^n$, where $n$ is a prime number.

Similarly, we can ask:

Problem (D). Let $f$ be a pseudo-prime transcendental meromorphic function and $p$ a polynomial of degree $\geq 3$, which has no quadratic right factor. Must $p(f(z))$ be pseudo-prime?

In [12], G.D. Song and J. Huang proposed the above problem and solved it for the case that $p(z) = z^n$ with $n$ being an odd number. We proved in [10] that it is true if $f$ is not of the form $H \circ q$, where $H$ is an entire periodic function and $q$ is a polynomial. One may try to solve Problem D for deg $p$ is odd first.

Finally, we ask whether the answer of Problem A is yes if both $f$ and $g$ are assumed to be transcendental?

References

ON THE COMPOSITION ...


[8] S.A. Lysenko, *On the functional equation f(p(z)) = g(q(z)), where p and q are “generalized” polynomials and f and g are meromorphic functions*, Izvestiya: Mathematics, 60 (1996), 89-110.


Received July 29, 1998 and revised October 28, 1998. This research was partially supported by a UGC grant of Hong Kong (project no. HKUST710/96P).

DEPARTMENT OF PURE MATHEMATICS AND MATHEMATICAL STATISTICS
UNIVERSITY OF CAMBRIDGE
16 MILL LANE, CAMBRIDGE CB2 1SB
ENGLAND
E-mail address: ntw@dpmms.cam.ac.uk

DEPARTMENT OF MATHEMATICS
HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY
CLEAR WATER BAY
KOWLOON, HONG KONG
CHINA
E-mail address: mayang@ust.hk