ACTA ARITHMETICA
168.2 (2015)

Explicit algebraic dependence formulae for infinite products related with Fibonacci and Lucas numbers

by

Hajime Kaneko (Tsukuba), Takeshi Kurosawa (Tokyo),
Yohei Tachiya (Hirosaki) and Taka-aki Tanaka (Yokohama)

1. Introduction. Let α and β be real algebraic numbers with $|\alpha| > 1$ and $\alpha\beta = -1$. Then the generalized Fibonacci numbers and Lucas numbers are expressed, respectively, as

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n \quad (n \geq 0). \tag{1.1}$$

If $\alpha = (1 + \sqrt{5})/2$, we have $U_n = F_n$ and $V_n = L_n$ $(n \geq 0)$, where $\{F_n\}_{n\geq 0}$ and $\{L_n\}_{n\geq 0}$ are the sequences of Fibonacci numbers and Lucas numbers defined, respectively, by $F_{n+2} = F_{n+1} + F_n$ $(n \geq 0)$, $F_0 = 0$, $F_1 = 1$ and by $L_{n+2} = L_{n+1} + L_n$ $(n \geq 0)$, $L_0 = 2$, $L_1 = 1$. Let $d \geq 2$ be an integer. In [2], the second, third, and fourth authors gave necessary and sufficient conditions for the infinite products

$$\prod_{\substack{k=1 \\ U_{d^k} \neq -a_i}}^{\infty} \left(1 + \frac{a_i}{U_{d^k}}\right) \quad (i = 1, \dots, m) \tag{1.2}$$

or

$$\prod_{\substack{k=1 \\ V_{d^k} \neq -a_i}}^{\infty} \left(1 + \frac{a_i}{V_{d^k}}\right) \quad (i = 1, \dots, m) \tag{1.3}$$

to be algebraically dependent, where a_i are non-zero rational integers. In this paper, we relax the condition on the non-zero rational integers $a_1, \dots, a_m$ to non-zero real algebraic numbers, which gives new cases where the infinite products (1.2) or (1.3) are algebraically dependent.

2010 *Mathematics Subject Classification*: Primary 11J85; Secondary 11J81, 11J91.
Key words and phrases: algebraic dependence, infinite products, Fibonacci numbers, Lucas numbers, Mahler's method.

DOI: 10.4064/aa168-2-5 © Instytut Matematyczny PAN, 2015

The algebraic independence of the infinite products above can be proved by using Mahler's method explained in Section 2; thereby, the algebraic dependence of the infinite products (1.3) with non-zero distinct real algebraic numbers $a_1, \ldots, a_m$ is reduced to the problem of determining whether the set of the roots of the quadratic polynomials $z^2 + a_i z + 1$ $(1 \le i \le m)$ and $z^2 + 1$ includes subsets described by a certain algorithm. If $|a_i| > 2$ $(1 \le i \le m)$, the method used in this paper is essentially similar to that of [2] dealing with the case where $a_1, \ldots, a_m$ are rational integers. If $a_1, \ldots, a_m$ are non-zero distinct real algebraic numbers including those with $|a_i| \le 2$, it can arise that the infinite products (1.3) which were not treated in [2] are algebraically dependent (see Examples 2–6 below). In such a case, we establish the algorithm of selecting dth roots to find subsets mentioned above whose elements distribute on the unit circle with certain symmetry. For this purpose, Lemmas 4.1 and 4.2 play a crucial role. The necessary and sufficient conditions given in Theorems 1.1 and 1.3 are useful to obtain explicit algebraic dependence relations between the infinite products (1.2) and (1.3), whose transcendence degrees are just one less than the numbers of the infinite products appearing in each relation (see Examples 1–6).

We introduce the following notation which will be needed throughout this paper. Let $d \ge 2$ be a fixed integer. For $\tau \in \mathbb{C}$ with $|\tau| = 1$ and $i = 0, 1, \ldots,$ define $\Omega_i(\tau) := \{z \in \mathbb{C} \mid z^{d^i} = \tau \text{ or } z^{d^i} = \overline{\tau}\}$. Here and in what follows, for any $\gamma \in \mathbb{C}$ we denote by $\overline{\gamma}$ the complex conjugate of γ. Moreover, for $S \subset \mathbb{C}$ we denote $\overline{S} := \{\overline{\gamma} \mid \gamma \in S\}$. Let $\zeta_m = \exp(2\pi\sqrt{-1}/m)$. For any fixed integer $k \ge 1$, let $S_k(\tau)$ be a non-empty subset of $\Omega_k(\tau)$ such that for any $\gamma \in S_k(\tau)$ the numbers $\zeta_d \gamma$ and $\overline{\gamma}$ belong to $S_k(\tau)$. Namely, $S_k(\tau)$ satisfies

$$S_k(\tau) = \zeta_d S_k(\tau) \quad \text{and} \quad S_k(\tau) = \overline{S_k(\tau)}. \tag{1.4}$$

For example, if $k = 3$, $d = 2$, and $\tau = 1$, we have $\Omega_3(1) = \{\zeta_8^j \mid 0 \le j \le 7\}$ and we can choose $S_3(1) = \{\pm\zeta_8, \pm\zeta_8^3\}$. Note that the following sets are determined depending only on $S_k(\tau)$:

$$\begin{aligned} \Lambda_i(\tau) &= \{\gamma^{d^{k-i}} \mid \gamma \in S_k(\tau)\} \subset \Omega_i(\tau) & (0 \le i \le k-1), \\ \Gamma_i(\tau) &= \{\gamma \in \Omega_i(\tau) \mid \gamma^d \in \Lambda_{i-1}(\tau)\} \setminus \Lambda_i(\tau) & (1 \le i \le k-1). \end{aligned}$$

Define

$$\mathcal{E}_k(\tau) = \Big(\bigcup_{i=1}^{k-1} \Gamma_i(\tau)\Big) \cup S_k(\tau), \quad \mathcal{F}_k(\tau) = \begin{cases} \mathcal{E}_k(\tau) \cup \{\tau, \overline{\tau}\} & \text{if } \tau \notin \mathcal{E}_k(\tau), \\ \mathcal{E}_k(\tau) \setminus \{\tau, \overline{\tau}\} & \text{otherwise.} \end{cases}$$

Note that $\mathcal{E}_1(\tau) = S_1(\tau)$. The main results of this paper are as follows:

THEOREM 1.1. *Let $\{U_n\}_{n \ge 0}$ be the sequence defined by* (1.1) *and d an integer greater than* 1. *Let $a_1, \ldots, a_m$ be non-zero distinct real algebraic num-*

bers. Then the numbers

$$\prod_{\substack{k=0\\ U_{d^k}\neq -a_i}}^{\infty}\left(1+\frac{a_i}{U_{d^k}}\right)\qquad (i=1,\ldots,m)$$

are algebraically dependent if and only if d is odd and there exist $\tau_1,\tau_2\in\mathbb{C}$ with $\tau_1\neq\tau_2$, $|\tau_1|=|\tau_2|=1$ and $\mathcal{F}_{k_1}(\tau_1),\mathcal{F}_{k_2}(\tau_2)$ with $k_1,k_2\geq 1$ such that $\mathcal{F}_{k_1}(\tau_1)\cap\mathcal{F}_{k_2}(\tau_2)\subset\{\tau_1,\overline{\tau_1},\tau_2,\overline{\tau_2}\}$ and $\{a_1,\ldots,a_m\}$ contains

$$-\frac{1}{\alpha-\beta}(\gamma+\overline{\gamma})$$

for all $\gamma\in(\mathcal{F}_{k_1}(\tau_1)\cup\mathcal{F}_{k_2}(\tau_2))\setminus\{\pm\sqrt{-1}\}$.

Corollary 1.2. *For any integer $d\geq 2$ and for any real algebraic number $a\neq 0$, the infinite product*

$$\prod_{\substack{k=0\\ U_{d^k}\neq -a}}^{\infty}\left(1+\frac{a}{U_{d^k}}\right)$$

is transcendental.

This follows from the fact that the algebraic dependence condition of Theorem 1.1 requires two non-empty sets $\mathcal{F}_{k_1}(\tau_1)$ and $\mathcal{F}_{k_2}(\tau_2)$. The transcendence of the numbers such as the infinite products in Corollary 1.2 was shown in [5].

Examples 1–6 below are obtained by using Theorems 1.1 and 1.3 of this paper. For the details, see [3].

Example 1. Let a be a non-zero real algebraic number. The transcendental numbers

$$s_1=\prod_{\substack{k=0\\ F_{3^k}\neq -a}}^{\infty}\left(1+\frac{a}{F_{3^k}}\right)\quad\text{and}\quad s_2=\prod_{\substack{k=0\\ F_{3^k}\neq a}}^{\infty}\left(1-\frac{a}{F_{3^k}}\right)$$

are algebraically dependent if and only if $a=\pm 1/\sqrt{5}$. If $a=1/\sqrt{5}$, then $s_1s_2^{-1}=2+\sqrt{5}$.

Theorem 1.3. *Let $\{V_n\}_{n\geq 0}$ be the sequence defined by (1.1) and d an integer greater than 1. Let $a_1,\ldots,a_m$ be non-zero distinct real algebraic numbers. Then the numbers*

$$\prod_{\substack{k=0\\ V_{d^k}\neq -a_i}}^{\infty}\left(1+\frac{a_i}{V_{d^k}}\right)\qquad (i=1,\ldots,m)\tag{1.5}$$

are algebraically dependent if and only if at least one of the following three properties is satisfied:

(i) $d = 2$ *and the set* $\{a_1, \ldots, a_m\}$ *contains* $b_1, \ldots, b_l$ $(l \geq 3)$ *satisfying*

$$b_1 < -2,\ b_2 = -b_1,\ b_j = b_{j-1}^2 - 2\ (j = 3, \ldots, l-1),\ b_l = -b_{l-1}^2 + 2.$$

(ii) $d = 2$ *and there exist* $\tau \in \mathbb{C}$ *with* $|\tau| = 1$ *and* $\mathcal{F}_k(\tau)$ *with* $k \geq 1$ *such that* $\{a_1, \ldots, a_m\}$ *contains* $-(\gamma + \overline{\gamma})$ *for all* $\gamma \in \mathcal{F}_k(\tau) \setminus \{\pm\sqrt{-1}\}$.

(iii) $d \geq 4$ *is even and there exist* $\tau_1, \tau_2 \in \mathbb{C}$ *with* $\tau_1 \neq \tau_2$, $|\tau_1| = |\tau_2| = 1$ *and* $\mathcal{F}_{k_1}(\tau_1), \mathcal{F}_{k_2}(\tau_2)$ *with* $k_1, k_2 \geq 1$ *such that* $\mathcal{F}_{k_1}(\tau_1) \cap \mathcal{F}_{k_2}(\tau_2) \subset \{\tau_1, \overline{\tau_1}, \tau_2, \overline{\tau_2}\}$ *and* $\{a_1, \ldots, a_m\}$ *contains* $-(\gamma + \overline{\gamma})$ *for all* $\gamma \in (\mathcal{F}_{k_1}(\tau_1) \cup \mathcal{F}_{k_2}(\tau_2)) \setminus \{\pm\sqrt{-1}\}$.

Remark 1.4. If $d = 2$, setting $\tau_1 = \zeta_3 = \zeta_6^2$, $S_1(\tau_1) = \{\zeta_6, \zeta_6^2, \zeta_6^4, \zeta_6^5\}$, $\tau_2 = -1$, and $S_1(\tau_2) = \{\sqrt{-1}, -\sqrt{-1}\}$, we have $\mathcal{F}_1(\tau_1) = \{\zeta_6, \zeta_6^5\}$ and $\mathcal{F}_1(\tau_2) = \{-1, \sqrt{-1}, -\sqrt{-1}\}$. Hence, using (ii) of Theorem 1.3 and noting that $-(\zeta_6 + \zeta_6^5) = -1$ and $-(-1-1) = 2$, we see that the corresponding infinite products (1.5) are algebraic numbers. Indeed,

$$\prod_{k=1}^{\infty}\left(1 - \frac{1}{V_{2^k}}\right) = \frac{\alpha^4 - 1}{\alpha^4 + \alpha^2 + 1} \quad \text{and} \quad \prod_{k=1}^{\infty}\left(1 + \frac{2}{V_{2^k}}\right) = \frac{\alpha^2 + 1}{\alpha^2 - 1}.$$

Corollary 1.5. *Let* $d \geq 2$ *be an integer and* $a \neq 0$ *be a real algebraic number with* $(d, a) \neq (2, -1), (2, 2)$. *Then the infinite product*

$$\prod_{\substack{k=0 \\ V_{d^k} \neq -a}}^{\infty} \left(1 + \frac{a}{V_{d^k}}\right)$$

is transcendental.

This corollary can be deduced from the following discussion: Case (iii) of Theorem 1.3 requires two non-empty sets $\mathcal{F}_{k_1}(\tau_1)$ and $\mathcal{F}_{k_2}(\tau_2)$. Hence, if $d \geq 4$, the infinite product in the corollary is transcendental. When $d = 2$, case (i) of Theorem 1.3 requires at least three numbers. Therefore only case (ii) has a possibility for the infinite product to be algebraic. If the number of elements in $\mathcal{F}_k(\tau) \setminus \{\pm\sqrt{-1}\}$ is at most two, the infinite product is algebraic, as is shown in Remark 1.4 above. The transcendence of the numbers such as the infinite products in the corollary was shown in [5].

Example 2. Let $a \neq \pm 1, \pm 2$ be a real algebraic number. The transcendental numbers

$$s_1 = \prod_{\substack{k=1 \\ L_{2^k} \neq -a}}^{\infty} \left(1 + \frac{a}{L_{2^k}}\right) \quad \text{and} \quad s_2 = \prod_{\substack{k=1 \\ L_{2^k} \neq a}}^{\infty} \left(1 - \frac{a}{L_{2^k}}\right)$$

are algebraically dependent if and only if $a = \pm\sqrt{2}$. If $a = \pm\sqrt{2}$, then $s_1 s_2 = \sqrt{5}/3$.

Example 3. The transcendental numbers

$$s_1=\prod_{k=1}^{\infty}\Bigl(1-\frac{\sqrt{3}}{L_{4^k}}\Bigr),\quad s_2=\prod_{k=1}^{\infty}\Bigl(1+\frac{\sqrt{3}}{L_{4^k}}\Bigr),$$
$$s_3=\prod_{k=1}^{\infty}\Bigl(1-\frac{1}{L_{4^k}}\Bigr),\quad s_4=\prod_{k=1}^{\infty}\Bigl(1+\frac{2}{L_{4^k}}\Bigr)$$

satisfy

$$s_1s_2s_3s_4^{-1}=\frac{5}{8},$$

while $\operatorname{trans.deg}_{\mathbb{Q}}\mathbb{Q}(s_1,s_2,s_3,s_4)=3$.

Example 4. The transcendental numbers

$$s_1=\prod_{k=1}^{\infty}\Bigl(1-\frac{1}{L_{6^k}}\Bigr),\quad s_2=\prod_{k=1}^{\infty}\Bigl(1+\frac{1}{L_{6^k}}\Bigr),\quad s_3=\prod_{k=1}^{\infty}\Bigl(1+\frac{2}{L_{6^k}}\Bigr),$$
$$s_4=\prod_{k=1}^{\infty}\Bigl(1+\frac{\sqrt{3}}{L_{6^k}}\Bigr),\quad s_5=\prod_{k=1}^{\infty}\Bigl(1-\frac{\sqrt{3}}{L_{6^k}}\Bigr)$$

satisfy

$$s_1s_2s_3s_4^{-1}s_5^{-1}=\frac{\sqrt{5}}{2},$$

while $\operatorname{trans.deg}_{\mathbb{Q}}\mathbb{Q}(s_1,s_2,s_3,s_4,s_5)=4$.

Example 5. The transcendental numbers

$$s_i=\prod_{k=1}^{\infty}\Bigl(1+\frac{a_i}{L_{4^k}}\Bigr)\qquad(i=1,\dots,8),$$

where

$a_1=-(\zeta_{16}^{1}+\zeta_{16}^{15})$, $a_2=-(\zeta_{16}^{5}+\zeta_{16}^{11})$, $a_3=-(\zeta_{16}^{7}+\zeta_{16}^{9})$, $a_4=-(\zeta_{64}^{3}+\zeta_{64}^{61})$, $a_5=-(\zeta_{64}^{13}+\zeta_{64}^{51})$, $a_6=-(\zeta_{64}^{19}+\zeta_{64}^{45})$, $a_7=-(\zeta_{64}^{29}+\zeta_{64}^{35})$, $a_8=2$,

satisfy

$$s_1s_2\cdots s_7s_8^{-2}=\frac{25}{7(7-\sqrt{2-\sqrt{2}})},$$

while $\operatorname{trans.deg}_{\mathbb{Q}}\mathbb{Q}(s_1,\dots,s_8)=7$.

Example 6. The transcendental numbers

$$s_i=\prod_{k=1}^{\infty}\Bigl(1+\frac{a_i}{L_{4^k}}\Bigr)\quad(i=1,\dots,10),$$

where

$$a_1 = -\frac{3}{2}, \quad a_2 = \frac{\sqrt{7}}{2}, \quad a_3 = \frac{3}{2}, \quad a_4 = -\frac{\sqrt{7}}{2}, \quad a_5 = \frac{31}{16},$$
$$a_6 = -\frac{4}{\sqrt{5}}, \quad a_7 = \frac{2}{\sqrt{5}}, \quad a_8 = \frac{4}{\sqrt{5}}, \quad a_9 = -\frac{2}{\sqrt{5}}, \quad a_{10} = \frac{14}{25},$$

satisfy

$$s_1 s_2 s_3 s_4 s_5^{-1} s_6^{-1} s_7^{-1} s_8^{-1} s_9^{-1} s_{10} = \frac{3024}{3575},$$

while $\operatorname{trans.deg}_{\mathbb{Q}} \mathbb{Q}(s_1, \ldots, s_{10}) = 9$.

The proofs of Theorems 1.1 and 1.3 will be given in Section 5.

2. Functional equations. In this section, we explain the Mahler method mentioned in the Introduction. Let $\boldsymbol{K}$ be an algebraic number field, $\boldsymbol{K}(z)$ the field of rational functions over $\boldsymbol{K}$, and $\boldsymbol{K}[[z]]$ the ring of formal power series with coefficients in $\boldsymbol{K}$. In what follows, let d be an integer greater than 1. We define the subgroup H_d of the multiplicative group $\boldsymbol{K}(z)^\times$ of non-zero elements of $\boldsymbol{K}(z)$ by

$$H_d := \left\{ \frac{g(z^d)}{g(z)} \,\middle|\, g(z) \in \boldsymbol{K}(z)^\times \right\}. \tag{2.1}$$

The functions $c_1(z), \ldots, c_m(z) \in \boldsymbol{K}(z)^\times$ are called *multiplicatively dependent modulo H_d* if there exist rational integers $e_1, \ldots, e_m$, not all zero, such that

$$\prod_{i=1}^{m} c_i(z)^{e_i} \in H_d.$$

If no such rational integers exist, then the functions $c_1(z), \ldots, c_m(z)$ are said to be *multiplicatively independent modulo H_d*.

We use the following lemmas for proving the theorems.

Lemma 2.1 (Kubota [1, Corollary 8]). *Let $f_1(z), \ldots, f_m(z) \in \boldsymbol{K}[[z]] \setminus \{0\}$ satisfy the functional equations*

$$f_i(z^d) = c_i(z) f_i(z), \quad c_i(z) \in \boldsymbol{K}(z)^\times \quad (i = 1, \ldots, m). \tag{2.2}$$

Then $f_1(z), \ldots, f_m(z)$ are algebraically independent over $\boldsymbol{K}(z)$ if and only if the rational functions $c_1(z), \ldots, c_m(z)$ are multiplicatively independent modulo H_d.

Lemma 2.2 (Kubota [1], see also Nishioka [4, Theorem 3.6.4]). *Suppose that $f_1(z), \ldots, f_m(z) \in \boldsymbol{K}[[z]]$ converge in $|z| < 1$ and satisfy the functional equations* (2.2) *with $c_i(0) \neq 0$. Let γ be an algebraic number with $0 < |\gamma| < 1$ such that $c_i(\gamma^{d^k})$ are defined and non-zero for all $k \geq 0$. If $f_1(z), \ldots, f_m(z)$ are algebraically independent over $\boldsymbol{K}(z)$, then the values $f_1(\gamma), \ldots, f_m(\gamma)$ are algebraically independent.*

Let $\{R_n\}_{n\geq 0}$ be the sequence $\{U_n\}_{n\geq 0}$ or $\{V_n\}_{n\geq 0}$ defined by (1.1). Then for any non-zero real algebraic numbers $a_1, \ldots, a_m$, we set

$$\Phi_i(z) = \prod_{k=0}^{\infty}\left(1 + \frac{p_i z^{d^k}}{1 + bz^{2d^k}}\right) \qquad (i = 1, \ldots, m),$$

where

$$(2.3) \qquad (p_i, b) = \begin{cases} ((\alpha-\beta)a_i, -(-1)^d) & \text{if } R_n = U_n, \\ (a_i, (-1)^d) & \text{if } R_n = V_n. \end{cases}$$

Taking an integer $N \geq 1$ such that $|R_{d^k}| > \max\{|a_1|, \ldots, |a_m|\}$ for all $k \geq N$ and noting that $\alpha\beta = -1$, we get

$$\begin{aligned} \Phi_i(\alpha^{-d^N}) &= \prod_{k=N}^{\infty}\left(1 + \frac{p_i \alpha^{-d^k}}{1 + b\alpha^{-2d^k}}\right) = \prod_{k=N}^{\infty}\left(1 + \frac{p_i}{\alpha^{d^k} + b(-1)^{d^k}\beta^{d^k}}\right) \\ &= \prod_{k=N}^{\infty}\left(1 + \frac{a_i}{R_{d^k}}\right) \qquad (i = 1, \ldots, m) \end{aligned}$$

so that

$$(2.4) \qquad \prod_{\substack{k=0 \\ R_{d^k} \neq -a_i}}^{\infty}\left(1 + \frac{a_i}{R_{d^k}}\right) = \Phi_i(\alpha^{-d^N}) \prod_{\substack{k=0 \\ R_{d^k} \neq -a_i}}^{N-1}\left(1 + \frac{a_i}{R_{d^k}}\right) \qquad (i = 1, \ldots, m).$$

Suppose that the numbers (2.4) are algebraically dependent. Then so are the values $\Phi_1(\alpha^{-d^N}), \ldots, \Phi_m(\alpha^{-d^N})$. Since $\Phi_1(z), \ldots, \Phi_m(z)$ satisfy the functional equations

$$(2.5) \qquad \Phi_i(z^d) = c_i(z)\Phi_i(z), \quad c_i(z) = \frac{1 + bz^2}{1 + p_i z + bz^2} \qquad (i = 1, \ldots, m),$$

the functions $\Phi_1(z), \ldots, \Phi_m(z)$ are algebraically dependent over $\boldsymbol{K}(z)$ by Lemma 2.2 with $\boldsymbol{K} = \mathbb{Q}(\alpha, a_1, \ldots, a_m)$. Then by Lemma 2.1 the rational functions $c_1(z), \ldots, c_m(z)$ are multiplicatively dependent modulo H_d, so there exist integers $e_1, \ldots, e_m$, not all zero, and $g(z) \in \boldsymbol{K}(z)^\times$ such that $\prod_{i=1}^{m} c_i(z)^{e_i} = g(z^d)/g(z)$. Then, renumbering the p_i, we may assume that there exist coprime polynomials $A(z), B(z) \in \boldsymbol{K}[z] \setminus \{0\}$ such that

$$(2.6) \qquad A(z^d)B(z)\prod_{i=1}^{k} P_i(z)^{e_i} = (1 + bz^2)^e A(z)B(z^d) \prod_{i=k+1}^{l} P_i(z)^{e_i},$$

where k, e_i, e are integers with $k, e_i \geq 1$, $e \geq 0$ and $P_i(z) = 1 + p_i z + bz^2$. We note that $\sum_{i=1}^{k} e_i = e + \sum_{i=k+1}^{l} e_i$.

We consider the functional equation (2.7) below, which is more general than (2.6). Let $P(z), Q(z) \in \mathbb{C}[z] \setminus \{0\}$ be coprime polynomials with $\deg P(z)Q(z) > 0$ satisfying

$$A(z^d)B(z)P(z) = A(z)B(z^d)Q(z), \tag{2.7}$$

where $d \geq 2$ is an integer and $A(z), B(z) \in \mathbb{C}[z] \setminus \{0\}$ are coprime. Note that the degrees of $P(z)$ and $Q(z)$ are not necessarily the same.

Let θ be a complex number and $\{\theta_n\}_{n\geq 1}$ a sequence of non-real numbers. We call $\{\theta_n\}_{n\geq 1}$ a *compatible non-real sequence of roots of* θ if $\theta_1^d = \theta$, $\theta_{n+1}^d = \theta_n$ for any $n \geq 1$, and the set $\{\theta_n \mid n \geq 1\}$ is infinite. In particular, $\theta_n^{d^n} = \theta$ for any $n \geq 1$.

Lemma 2.3. *Assume that $P(z)$ and $Q(z)$ satisfy* (2.7). *Let $\theta \in \mathbb{C}$.*

(i) *Suppose that there exists a compatible non-real sequence $\{\theta_n\}_{n\geq 1}$ of roots of θ satisfying $Q(\theta_n) \neq 0$ (resp. $P(\theta_n) \neq 0$) for any $n \geq 1$. Then $A(\theta) \neq 0$ (resp. $B(\theta) \neq 0$).*

(ii) *Let l be a positive integer. Assume that $Q(\theta^{d^n}) \neq 0$ for any n with $1 \leq n \leq l$ and that $B(\theta^d) = 0$. Then $B(\theta^{d^n}) = 0$ for any n with $1 \leq n \leq l+1$.*

(iii) *Suppose $Q(\theta^{d^n}) \neq 0$ for any $n \geq 1$ and the set $\{\theta^{d^n} \mid n \geq 1\}$ is infinite. Then $B(\theta^d) \neq 0$.*

Proof. For the proof of (i) we only check the case of

$$Q(\theta_n) \neq 0 \quad (n \geq 1) \tag{2.8}$$

since that of $P(\theta_n) \neq 0$ $(n \geq 1)$ is proved by the symmetry of (2.7). Suppose on the contrary that $A(\theta) = 0$. By (2.8) and the fact that $A(z)$ and $B(z)$ are coprime, $B(\theta)Q(\theta_1) \neq 0$. Thus, substituting $z = \theta_1$ into (2.7), we get $A(\theta_1) = 0$ because $\theta_1^d = \theta$. Next suppose that $A(\theta_n) = 0$ for some $n \geq 1$. In the same way as above, $B(\theta_n)Q(\theta_{n+1}) \neq 0$. Since $\theta_{n+1}^d = \theta_n$, putting $z = \theta_{n+1}$ into (2.7), we see that $A(\theta_{n+1}) = 0$. Hence $A(\theta_n) = 0$ for any $n \geq 1$, which is impossible since the set $\{\theta_n \mid n \geq 1\}$ is infinite and $A(z)$ is a polynomial. This completes the proof of (i).

Next we show (ii) by induction on n. The case of $n = 1$ is trivial. Suppose that $B(\theta^{d^n}) = 0$ for some n with $1 \leq n \leq l$. Then $A(\theta^{d^n})Q(\theta^{d^n}) \neq 0$ since $A(z)$ and $B(z)$ are coprime. Thus, substituting $z = \theta^{d^n}$ into (2.7), we get $B(\theta^{d^{n+1}}) = 0$, and (ii) is proved.

Statement (iii) follows from (ii) since $B(z)$ is a polynomial. ∎

3. The case where $P(z)$ and $Q(z)$ are products of quadratic polynomials. Let $\boldsymbol{K} \subset \mathbb{R}$ be an algebraic number field. In this section, we consider the special case of $P(z)$ and $Q(z)$ involving (2.6), namely, $P(z), Q(z)$

are expressed as

$$(3.1)\qquad P(z)=\prod_{i=1}^{s}(1+p_iz+bz^2),\qquad Q(z)=\prod_{j=s+1}^{t}(1+q_jz+bz^2)$$

with $b=\pm1$ and $p_i\neq q_j$ for all i,j and $P(z),Q(z)$ satisfy the functional equation (2.7) with $A(z),B(z)\in \boldsymbol{K}[z]\setminus\{0\}$. Note that $p_1,\ldots,p_s$ are not necessarily distinct and neither are $q_{s+1},\ldots,q_t$. First we show $b=1$ in Lemma 3.2 below, and then we investigate the properties of $P(z)$ and $Q(z)$ in different situations (see Subsections 3.1 and 3.2).

Suppose that $P(z)Q(z)$ has real roots. Let α_1 be one of these with the largest absolute value, so $\alpha_1\in\mathbb{R}$ satisfies $P(\alpha_1)Q(\alpha_1)=0$ and

$$(3.2)\qquad |\alpha_1|=\max\{|\gamma|\mid \gamma\in\mathbb{R},\ P(\gamma)Q(\gamma)=0\}.$$

Then, exchanging $A(z)$ and $B(z)$ in (2.7) if necessary, we may assume that

$$P(\alpha_1)=0.$$

By (3.1), $\beta_1:=(b\alpha_1)^{-1}$ satisfies $P(\beta_1)=0$ and the absolute value of β_1 is the smallest among those of the real roots of $P(z)Q(z)$. Comparing the orders at $z=1$ of both sides of (2.7), we obtain $P(1)Q(1)\neq0$, which yields $\alpha_1,\beta_1\neq1$.

LEMMA 3.1. *Let $P(z)$ and $Q(z)$ be polynomials of the form* (3.1) *which satisfy* (2.7). *If the roots of $P(z)Q(z)$ are real, then $A(z)B(z)$ has no negative root.*

Proof. For any negative number θ, there exists a compatible non-real sequence $\{\theta_n\}_{n\geq1}$ of roots of θ. We see that $P(\theta_n)Q(\theta_n)\neq0$ for any $n\geq1$ by the assumption of the lemma. Thus $A(\theta)B(\theta)\neq0$ by Lemma 2.3(i). Since θ is any negative number, the lemma is proved. ∎

LEMMA 3.2. *If $b=-1$, then there are no polynomials $A(z)$ and $B(z)$ of the form* (3.1) *which satisfy* (2.7).

Proof. Since $b<0$, the roots of $P(z)Q(z)$ are real. By the definition of α_1 and β_1, we have $\alpha_1\beta_1=-1$. Hence $\alpha_1<-1$ or $-1<\beta_1<0$ because $\alpha_1,\beta_1\neq1$. Suppose that $\alpha_1<-1$. Then $Q(\alpha_1^{d^n})\neq0$ for any $n\geq1$ by (3.2). Substituting $z=\alpha_1$ into (2.7), we get $A(\alpha_1)B(\alpha_1^d)=0$, which is a contradiction since $A(\alpha_1)\neq0$ by Lemma 3.1 and $B(\alpha_1^d)\neq0$ by Lemma 2.3(iii). Similarly we deduce a contradiction in the case of $-1<\beta_1<0$, using the fact that $|\beta_1|$ is the smallest modulus among the roots of $P(z)Q(z)$. ∎

By Lemma 3.2, we have $b=1$. Hence we need only consider the equation

$$(3.3)\qquad A(z^d)B(z)P(z)=A(z)B(z^d)Q(z),$$

where $A(z), B(z) \in \boldsymbol{K}[z] \setminus \{0\}$ are coprime and

$$P(z) = \prod_{i=1}^{s}(1 + p_i z + z^2), \qquad Q(z) = \prod_{j=s+1}^{t}(1 + q_j z + z^2)$$

with $p_i \neq q_j$ for all i, j.

3.1. The case where $d = 2$ and $P(z)Q(z)$ has real roots. In this subsection, we consider equation (3.3) where $d = 2$ and $P(z)Q(z)$ has real roots.

Lemma 3.3. *Let $P(z)$ and $Q(z)$ be polynomials satisfying* (3.3) *with $d = 2$. Suppose that $P(z)Q(z)$ has a real root $\alpha_1 < 0$ with* (3.2). *Then $\alpha_1 = -1$.*

Proof. First we note that the non-real roots of $P(z)Q(z)$ are of absolute value 1, since $P(z)Q(z)$ is the product of quadratic self-reciprocal polynomials. Assume that $\alpha_1 \neq -1$. Since $\alpha_1 < 0$ and $\beta_1 = \alpha_1^{-1}$, we get $|\alpha_1| > 1 > |\beta_1|$, and so $Q(\alpha_1^{2^n}) \neq 0$ for any $n \geq 0$ by (3.2) and the fact that $P(z)$ and $Q(z)$ are coprime. Substituting $z = \alpha_1$ into (3.3), we get $A(\alpha_1) = 0$, because $B(\alpha_1^2) \neq 0$ by Lemma 2.3(iii).

On the other hand, there exists a compatible non-real sequence $\{\theta_n\}_{n\geq 1}$ of roots of α_1 because $\alpha_1 < 0$. Hence we see that $Q(\theta_n) \neq 0$ for any $n \geq 1$ by $|\theta_n| > 1$. By Lemma 2.3(i) we get $A(\alpha_1) \neq 0$, which is a contradiction. Therefore $\alpha_1 = \beta_1 = -1$. ∎

Lemma 3.4. *Let $P(z)$ and $Q(z)$ be polynomials satisfying* (3.3) *with $d = 2$. Suppose that $P(z)Q(z)$ has a real root $\alpha_1 > 0$ with* (3.2). *Then there exist $k \geq 1$ and $\alpha, \beta \in \mathbb{R}$ with $\alpha_1 = \alpha^{2^k}$ and $\beta = \alpha^{-1}$ such that $P(z)$, $Q(z)$, and $A(z)$ are divisible respectively by*

$$(3.4)\qquad \begin{gathered}(z - \alpha^{2^k})(z - \beta^{2^k}), \quad (z-\alpha)(z-\beta)\prod_{i=0}^{k-1}(z + \alpha^{2^i})(z + \beta^{2^i}), \quad \textit{and} \\ \prod_{i=1}^{k}(z - \alpha^{2^i})(z - \beta^{2^i}).\end{gathered}$$

Proof. Consider the positive 2^jth roots $\alpha_1^{2^{-j}}, \beta_1^{2^{-j}}$ for any integer $j \geq 1$. Note that $\alpha_1 > 1$. We first show that $A(-\alpha_1^{2^{-j}}) \neq 0$ for any $j \geq 1$. Suppose on the contrary that $A(-\alpha_1^{2^{-j}}) = 0$ for some $j \geq 1$. Then there exists an integer $l \geq 1$ such that, for $\theta := (-\alpha_1^{2^{-j}})^{2^{-l}} \in \mathbb{C} \setminus \mathbb{R}$, we have $A(\theta^2) = 0$ and $A(\theta) \neq 0$ since $A(z)$ is a polynomial. Substituting $z = \theta$ into (3.3) with $d = 2$, we obtain $Q(\theta) = 0$, which is impossible with $|\theta| > 1$, since $Q(z)$ is the product of quadratic self-reciprocal polynomials, and so its non-real roots are of absolute value 1.

If there exists an integer $i \geq 1$ satisfying $Q(\alpha_1^{2^{-i}}) = 0$, we denote the minimal such i by k. Otherwise, we let $k = \infty$. We verify

$$A(\alpha_1^{2^{-j}}) = 0 \quad (0 \leq j \leq k-1)$$

by induction on j, which implies that $k < \infty$ since $A(z)$ is a polynomial. For $j = 0$ we substitute $z = \alpha_1$ into (3.3) with $d = 2$. Then $A(\alpha_1) = 0$ because $B(\alpha_1^2) \neq 0$ by (3.2) and Lemma 2.3(iii). Next we show that $A(\alpha_1^{2^{-j}}) = 0$ for $1 \leq j \leq k-1$ under the assumption that $A(\alpha_1^{2^{-(j-1)}}) = 0$. Then $B(\alpha_1^{2^{-j+1}}) \neq 0$ and by the minimality of k we have $Q(\alpha_1^{2^{-j}}) \neq 0$. Substituting $z = \alpha_1^{2^{-j}}$ into (3.3), we obtain $A(\alpha_1^{2^{-j}}) = 0$.

We see that k is the minimal integer such that $Q(\beta_1^{2^{-k}}) = 0$ because $\beta_1 = \alpha_1^{-1}$ and $Q(z)$ is self-reciprocal. In the same way as in the preceding paragraph, we obtain $A(\beta_1^{2^{-j}}) = 0$ for $0 \leq j \leq k-1$. Letting $\alpha := \alpha_1^{2^{-k}}$ and $\beta := \alpha^{-1} = \beta_1^{2^{-k}}$, we see that $P(z)$ and $A(z)$ are divisible by the corresponding polynomials in (3.4). For any $1 \leq j \leq k$, substituting $z = -\alpha_1^{2^{-j}}$ into (3.3), we get $Q(-\alpha_1^{2^{-j}}) = 0$ since $A(\alpha_1^{2^{-j+1}}) = 0$, $B(\alpha_1^{2^{-j+1}}) \neq 0$, and $A(-\alpha_1^{2^{-j}}) \neq 0$ by the first paragraph of the proof. Observing that $Q(\alpha_1^{2^{-k}}) = 0$ and that $\beta_1 = \alpha_1^{-1}$ and $Q(z)$ is self-reciprocal, we have verified the lemma. ∎

Remark 3.5. Let $P(z)$ and $Q(z)$ be polynomials satisfying (3.3) with $d = 2$ and let α, β be as in Lemma 3.4. Then $P(z)$ and $Q(z)$ are divisible by

$$z^2 + b_{k+2}z + 1 \quad \text{and} \quad \prod_{i=1}^{k+1}(z^2 + b_i z + 1),$$

respectively, where $k \geq 1$ and

$$\begin{aligned} b_1 &= -(\alpha+\beta) < -2\sqrt{\alpha\beta} = -2, \\ b_2 &= \alpha + \beta = -b_1, \\ b_i &= \alpha^{2^{i-2}} + \beta^{2^{i-2}} = (\alpha^{2^{i-3}} + \beta^{2^{i-3}})^2 - 2 = b_{i-1}^2 - 2 \quad (3 \leq i \leq k+1), \\ b_{k+2} &= -(\alpha^{2^k} + \beta^{2^k}) = -b_{k+1}^2 + 2. \end{aligned}$$

3.2. The case where $d \geq 3$ or $P(z)Q(z)$ has no real roots. First we consider equation (3.3) in the case where $P(z)Q(z)$ has no real roots. Since $P(z)Q(z)$ is the product of quadratic self-reciprocal polynomials, the roots of $P(z)Q(z)$ are in the set

$$\mathcal{M} := \{\omega \in \mathbb{C} \mid |\omega| = 1, \, \omega \neq 1\}. \tag{3.5}$$

In the case of $d \geq 3$ we have the following:

Lemma 3.6. *Let $P(z)$ and $Q(z)$ be polynomials satisfying* (3.3). *If $d \geq 3$, then the roots of $P(z)Q(z)$ are in $\mathcal{M}$.*

Proof. Suppose that $P(z)Q(z)$ has real roots and let α_1 ($\neq 1$) be a real root of $P(z)$ as in (3.2). Assume that $\alpha_1 \neq -1$. Then $|\alpha_1| > 1 > |\beta_1|$. As in the proof of Lemma 3.3, we deduce a contradiction for $d \geq 3$ since there exists a compatible non-real sequence $\{\theta_n\}_{n\geq 1}$ of roots of α_1. ∎

In any case stated above, the roots of $P(z)Q(z)$ are continued in $\mathcal{M}$. In the next section we investigate such a case for more general polynomials $P(z)$ and $Q(z)$.

4. The case where $P(z)Q(z)$ has roots in $\mathcal{M}$. Let $P(z)$ and $Q(z)$ be non-zero coprime polynomials with complex coefficients satisfying (2.7). We note that $P(z)$ and $Q(z)$ are not necessarily products of quadratic polynomials. In this section, assume that $P(z)Q(z)$ has roots in $\mathcal{M}$. Let $\alpha \in \mathbb{C}$ with $|\alpha| = 1$ be the root of $P(z)Q(z)$ having the smallest positive argument among its roots in $\mathcal{M}$. Without loss of generality, we may assume that $P(\alpha) = 0$ and $Q(\alpha) \neq 0$. Substituting $z = \alpha$ into (2.7), we get $A(\alpha)B(\alpha^d) = 0$. Taking a compatible non-real sequence $\{\theta_n\}_{n\geq 1}$ of roots of α satisfying $0 < \arg(\theta_n) < \arg(\alpha)$ for any $n \geq 1$, we get $Q(\theta_n) \neq 0$, and so $A(\alpha) \neq 0$ by Lemma 2.3(i). Therefore

$$B(\alpha^d) = 0. \tag{4.1}$$

In this section we calculate the factors of $B(z)$, $P(z)$, and $Q(z)$. First we consider the case where $Q(\alpha^{d^m}) = 0$ for some $m \geq 1$, which corresponds to Lemma 4.1 below. Next we treat the case where $Q(\alpha^{d^m}) \neq 0$ for any integer $m \geq 1$, which corresponds to Lemma 4.2. We introduce the following notation. For $\tau \in \mathbb{C}$ with $|\tau| = 1$, set

$$\Theta_i(\tau) := \{\gamma \in \mathbb{C} \mid \gamma^{d^i} = \tau\} \quad (i = 0, 1, \ldots).$$

We note that if $\pm 1 \in \Theta_i(\tau)$ for some $i \geq 0$, then $\tau = \pm 1$.

Let $k \geq 1$ be an integer and $M_k(\tau)$ a subset of $\Theta_k(\tau)$ satisfying $M_k(\tau) = \zeta_d M_k(\tau)$. For any given $M_k(\tau)$ the following sets are uniquely determined:

$$\begin{aligned} N_i(\tau) &= \{\gamma^{d^{k-i}} \mid \gamma \in M_k(\tau)\} \subset \Theta_i(\tau) && (0 \leq i \leq k-1),\\ M_i(\tau) &= \{\gamma \in \Theta_i(\tau) \mid \gamma^d \in N_{i-1}(\tau)\} \setminus N_i(\tau) && (1 \leq i \leq k-1),\end{aligned}$$

$$\tilde{\mathcal{E}}_k(\tau) = \bigcup_{i=1}^{k} M_i(\tau), \qquad \tilde{\mathcal{F}}_k(\tau) = \begin{cases} \tilde{\mathcal{E}}_k(\tau) \cup \{\tau\} & \text{if } \tau \notin \tilde{\mathcal{E}}_k(\tau),\\ \tilde{\mathcal{E}}_k(\tau) \setminus \{\tau\} & \text{otherwise.}\end{cases}$$

We observe that

$$N_0(\tau) = \{\tau\}. \tag{4.2}$$

Moreover, we use the notation

$$N_i^{1/d}(\tau) := \{\gamma \in \mathbb{C} \mid \gamma^d \in N_i(\tau)\}$$

in the proof of Lemmas 4.1 and 4.2.

Let $F^{(\tau)}(z)$ be a polynomial defined by

$$F^{(\tau)}(z) = \prod_{\gamma\in M_1(\tau)} (z-\gamma)\cdots \prod_{\gamma\in M_k(\tau)} (z-\gamma).$$

LEMMA 4.1. *Let $P(z)$ and $Q(z)$ satisfy (2.7). Let $\alpha \in \mathbb{C}$ with $|\alpha| = 1$ be the root of $P(z)Q(z)$ with the smallest positive argument among its roots in $\mathcal{M}$. Assume that $P(\alpha) = 0$ and $Q(\alpha^{d^m}) = 0$ for some integer $m \geq 1$. Then there exist $k \geq 1$, $\tau \in \mathbb{C}$ with $|\tau| = 1$, and $M_k(\tau)$ with $\tau \notin \tilde{\mathcal{E}}_k(\tau)$ such that $P(z)$ and $Q(z)$ are divisible by $F^{(\tau)}(z)$ and $z-\tau$, respectively.*

Proof. Let $s \geq 1$ be an integer such that $Q(\alpha^{d^s}) = 0$ and $Q(\alpha^{d^j}) \neq 0$ for $j = 0, 1, \dots, s-1$. Then $B(\alpha^{d^{j+1}}) = 0$ for $j = 0, 1, \dots, s-1$ by (4.1) and Lemma 2.3(ii). Setting $\tau = \alpha^{d^s}$, we have $|\tau| = 1$, $B(\tau) = 0$, and $A(\tau) \neq 0$. We give an algorithm to find $M_k(\tau)$, defining $M_i(\tau)$ and $N_i(\tau)$ below for $i = 1, \dots, k$ inductively.

Let

$$B_1(z) := \frac{B(z)}{z-\tau} \in \mathbb{C}[z] \quad \text{and} \quad Q_1(z) := \frac{Q(z)}{z-\tau} \in \mathbb{C}[z].$$

Then

$$A(z^d)B_1(z)P(z) = (z^d-\tau)A(z)B_1(z^d)Q_1(z). \tag{4.3}$$

Define

$$N_1(\tau) := \{\gamma \in \Theta_1(\tau) \mid B_1(\gamma) = 0\} \quad \text{and} \quad M_1(\tau) := \{\gamma \in \Theta_1(\tau) \mid B_1(\gamma) \neq 0\}.$$

Note that $\Theta_1(\tau) = N_1(\tau) \cup M_1(\tau)$ and $N_1(\tau) \cap M_1(\tau) = \emptyset$. Substituting $z = \gamma \in \Theta_1(\tau)$ into (4.3), we get $B_1(\gamma)P(\gamma) = 0$ because $A(\gamma^d) = A(\tau) \neq 0$. Hence, letting

$$B_2(z) := \frac{B_1(z)}{\prod_{\gamma\in N_1(\tau)}(z-\gamma)} \quad \text{and} \quad P_1(z) := \frac{P(z)}{\prod_{\gamma\in M_1(\tau)}(z-\gamma)} \in \mathbb{C}[z],$$

we see that

$$\begin{aligned} A(z^d)\Big(B_2(z)\prod_{\gamma\in N_1(\tau)}(z-\gamma)\Big)\Big(P_1(z)\prod_{\gamma\in M_1(\tau)}(z-\gamma)\Big) \\ = (z^d-\tau)A(z)\Big(B_2(z^d)\prod_{\gamma\in N_1(\tau)}(z^d-\gamma)\Big)Q_1(z). \end{aligned} \tag{4.4}$$

Noting that

$$\prod_{\gamma\in N_1(\tau)}(z-\gamma)\prod_{\gamma\in M_1(\tau)}(z-\gamma) = z^d-\tau$$

and dividing both sides of (4.4) by $z^d-\tau$, we get

$$A(z^d)B_2(z)P_1(z) = A(z)B_2(z^d)Q_1(z)\prod_{\gamma\in N_1(\tau)}(z^d-\gamma). \tag{4.5}$$

If $N_1(\tau)=\emptyset$, then $\Theta_1(\tau)=M_1(\tau)$, and hence $M_1(\tau)=\zeta_d M_1(\tau)$. Otherwise, for any $\gamma\in N_1^{1/d}(\tau)$, we have $B_1(\gamma^d)=0$, and hence $A(\gamma^d)\neq 0$. Then, substituting $z=\gamma\in N_1^{1/d}(\tau)$ into (4.5), we get $B_2(\gamma)P_1(\gamma)=0$. Define

$$N_2(\tau):=\{\gamma\in N_1^{1/d}(\tau)\mid B_2(\gamma)=0\},$$
$$M_2(\tau):=\{\gamma\in N_1^{1/d}(\tau)\mid B_2(\gamma)\neq 0\}.$$

We note that $N_1^{1/d}(\tau)=N_2(\tau)\cup M_2(\tau)$ and $N_2(\tau)\cap M_2(\tau)=\emptyset$. Hence, setting

$$B_3(z):=\frac{B_2(z)}{\prod_{\gamma\in N_2(\tau)}(z-\gamma)}\quad\text{and}\quad P_2(z):=\frac{P_1(z)}{\prod_{\gamma\in M_2(\tau)}(z-\gamma)}\in\mathbb{C}[z],$$

we have

$$(4.6)\qquad A(z^d)\Big(B_3(z)\prod_{\gamma\in N_2(\tau)}(z-\gamma)\Big)\Big(P_2(z)\prod_{\gamma\in M_2(\tau)}(z-\gamma)\Big) = A(z)\Big(B_3(z^d)\prod_{\gamma\in N_2(\tau)}(z^d-\gamma)\Big)Q_1(z)\prod_{\gamma\in N_1(\tau)}(z^d-\gamma).$$

Dividing both sides of (4.6) by

$$\prod_{\gamma\in N_2(\tau)}(z-\gamma)\prod_{\gamma\in M_2(\tau)}(z-\gamma)=\prod_{\gamma\in N_1(\tau)}(z^d-\gamma),$$

we get

$$A(z^d)B_3(z)P_2(z)=A(z)B_3(z^d)Q_1(z)\prod_{\gamma\in N_2(\tau)}(z^d-\gamma).$$

If $N_2(\tau)=\emptyset$, then $N_1^{1/d}(\tau)=M_2(\tau)$, and hence $\zeta_d M_2(\tau)=M_2(\tau)$. Otherwise, in the same way as above, we have

$$A(z^d)B_4(z)P_3(z)=A(z)B_4(z^d)Q_1(z)\prod_{\gamma\in N_3(\tau)}(z^d-\gamma).$$

We repeat this process, which terminates in a finite number of steps since $B(z)$ is a polynomial. Namely, there exists $k\geq 1$ such that $N_k(\tau)=\emptyset$, and so $N_{k-1}^{1/d}(\tau)=M_k(\tau)$. This implies $M_k(\tau)=\zeta_d M_k(\tau)$ and

$$A(z^d)B_{k+1}(z)P_k(z)=A(z)B_{k+1}(z^d)Q_1(z).$$

Since $P(z)$ and $Q(z)$ are coprime and $Q(\tau)=0$, we deduce that $\tau\notin\tilde{\mathcal{E}}_k(\tau)$. This completes the proof of Lemma 4.1. ∎

LEMMA 4.2. *Let $P(z)$ and $Q(z)$ satisfy* (2.7). *Let $\alpha\in\mathbb{C}$ with $|\alpha|=1$ be the root of $P(z)Q(z)$ with the smallest positive argument among its roots in $\mathcal{M}$. Assume that $P(\alpha)=0$ and $Q(\alpha^{d^m})\neq 0$ for any integer $m\geq 1$. Then* *there exist* $k \geq 1$, $\tau \in \mathbb{C}$ *with* $|\tau| = 1$, *and* $M_k(\tau)$ *with* $\tau \in \tilde{\mathcal{E}}_k(\tau)$ *such that* $P(z)$ *is divisible by* $F^{(\tau)}(z)/(z-\tau)$.

Proof. We give an algorithm to find $M_k(\tau)$, defining $M_i(\tau)$ and $N_i(\tau)$ below for $i = 1, \ldots, k$ inductively. We see that $B(\alpha^{d^m}) = 0$ for any $m \geq 1$ by (4.1) and Lemma 2.3(ii). Hence there exist integers r, s with $1 \leq r < s$ such that $\alpha^{d^r} = \alpha^{d^s}$, since $B(z)$ is a polynomial. We take the smallest $l = s - r \geq 1$. Note that $B(\alpha^{d^{r+1}}) = B(\alpha^{d^{r+2}}) = \cdots = B(\alpha^{d^s}) = 0$. Set $\tau := \alpha^{d^r} = \alpha^{d^s}$. Since $Q(\tau) \neq 0$, we need the following discussion different from the proof of Lemma 4.1.

Set

$$B_0(z) := B(z), \quad B_1(z) := \frac{B(z)}{z-\tau} \in \mathbb{C}[z], \quad \text{and} \quad P_0^{\dagger}(z) := (z-\tau)P(z).$$

For $i = 1, \ldots, l-1$ we define the sets $N_i(\tau), M_i(\tau) \subset \Theta_i(\tau)$ and the polynomials $B_{i+1}(z)$ and $P_i^{\dagger}(z)$, which are factors of $B(z)$ and $(z-\tau)P(z)$, respectively. Hence $A(z)$ and $B_i(z)$ are coprime for $i = 0, 1, \ldots, l$. To proceed with the induction, we simultaneously check the following for $i = 0, 1, \ldots, l-1$:

(i) For any $\gamma \in N_i(\tau)$ we have

$$B_i(\gamma) = 0. \tag{4.7}$$

(ii) We have

$$\alpha^{d^{s-i}} \in N_i(\tau). \tag{4.8}$$

In particular, $N_i(\tau) \neq \emptyset$.

(iii) It follows that

$$A(z^d)B_{i+1}(z)P_i^{\dagger}(z) = A(z)B_{i+1}(z^d)Q(z) \prod_{\gamma \in N_i(\tau)} (z^d - \gamma). \tag{4.9}$$

First, (4.7) and (4.8) with $i = 0$ are clear by (4.2). From (2.7) we have

$$A(z^d)B_1(z)P_0^{\dagger}(z) = A(z)B_1(z^d)Q(z)(z^d - \tau),$$

which implies (4.9) with $i = 0$.

Suppose that there exists an integer j with $1 \leq j \leq l-1$ such that $N_i(\tau)$, $B_{i+1}(z)$, and $P_i^{\dagger}(z)$ satisfy (4.7)–(4.9) for $i = 0, 1, \ldots, j-1$. Set

$$N_j(\tau) := \{\gamma \in N_{j-1}^{1/d}(\tau) \mid B_j(\gamma) = 0\},$$
$$M_j(\tau) := \{\gamma \in N_{j-1}^{1/d}(\tau) \mid B_j(\gamma) \neq 0\}.$$

Then (4.7) holds for $i = j$. Since $N_{j-1}^{1/d}(\tau) \subset \Theta_j(\tau)$ by $N_{j-1}(\tau) \subset \Theta_{j-1}(\tau)$, we get $N_j(\tau), M_j(\tau) \subset \Theta_j(\tau)$. For any $\gamma \in N_{j-1}^{1/d}(\tau)$, we have $B_{j-1}(\gamma^d) = 0$ by (4.7) with $i = j-1$, and so $A(\gamma^d) \neq 0$ since $B_{j-1}(z)$ and $A(z)$ are coprime. Thus, substituting $z = \gamma \in N_{j-1}^{1/d}(\tau)$ into (4.9) with $i = j-1$, we get $B_j(\gamma)P^{\dagger}_{j-1}(\gamma) = 0$. In particular, all the elements of the set $M_j(\tau)$ are the roots of $P^{\dagger}_{j-1}(z)$. Define

$$B_{j+1}(z) := \frac{B_j(z)}{\prod_{\gamma\in N_j(\tau)}(z-\gamma)} \in \mathbb{C}[z],$$

$$P^{\dagger}_j(z) := \frac{P^{\dagger}_{j-1}(z)}{\prod_{\gamma\in M_j(\tau)}(z-\gamma)} \in \mathbb{C}[z].$$

Note that $\alpha^{d^{s-j}} \in N^{1/d}_{j-1}(\tau)$ by (4.8) with $i = j-1$ and

$$B_j(z) = \frac{B(z)}{\prod_{i=0}^{j-1}\prod_{\gamma\in N_i(\tau)}(z-\gamma)}.$$

Recall that $B(\alpha^{d^{s-j}}) = 0$. For the proof of (4.8) with $i = j$, it suffices to show that $\alpha^{d^{s-j}} \notin N_h(\tau)$ for any $h = 0, 1, \ldots, j-1$. Suppose on the contrary that $\alpha^{d^{s-j}} \in N_h(\tau) \subset \Theta_h(\tau)$. Then $\alpha^{d^{s-j+h}} = \tau = \alpha^{d^s}$, which contradicts the minimality of l. Hence we showed (4.8) with $i = j$. We rewrite (4.9) with $i = j-1$ as

$$\begin{aligned} A(z^d)\Big(B_{j+1}(z)\prod_{\gamma\in N_j(\tau)}(z-\gamma)\Big)\Big(P^{\dagger}_j(z)\prod_{\gamma\in M_j(\tau)}(z-\gamma)\Big) \\ = A(z)\Big(B_{j+1}(z^d)\prod_{\gamma\in N_j(\tau)}(z^d-\gamma)\Big)Q(z)\prod_{\gamma\in N_{j-1}(\tau)}(z^d-\gamma). \end{aligned}$$

Dividing both sides of this equality by

$$\prod_{\gamma\in N_j(\tau)}(z-\gamma)\prod_{\gamma\in M_j(\tau)}(z-\gamma) = \prod_{\gamma\in N_{j-1}(\tau)}(z^d-\gamma),$$

we get

$$A(z^d)B_{j+1}(z)P^{\dagger}_j(z) = A(z)B_{j+1}(z^d)Q(z)\prod_{\gamma\in N_j(\tau)}(z^d-\gamma),$$

which implies (4.9) with $i = j$. Therefore, we have defined $N_i(\tau), M_i(\tau)$, $B_{i+1}(z)$, and $P^{\dagger}_i(z)$ for $i = 1, \ldots, l-1$.

We show that $z-\tau$ divides both $\prod_{\gamma\in N_{l-1}(\tau)}(z^d-\gamma)$ and

$$P^{\dagger}_{l-1}(z) = \frac{(z-\tau)P(z)}{\prod_{i=1}^{l-1}\prod_{\gamma\in M_i(\tau)}(z-\gamma)}.$$

First by (4.8) with $i = l-1$ we have

$$\tau^d = \alpha^{d^{r+1}} = \alpha^{d^{s-(l-1)}} \in N_{l-1}(\tau). \tag{4.10}$$

Hence $z-\tau$ divides $\prod_{\gamma\in N_{l-1}(\tau)}(z^d-\gamma)$. Next if $P^{\dagger}_{l-1}(\tau) \neq 0$, then we have

$\tau \in M_i(\tau) \subset \Theta_i(\tau)$ for some i with $1 \le i \le l-1$, and so $\tau^{d^i} = \tau$, which contradicts the minimality of l. Dividing both sides of (4.9) with $i = l-1$ by $z - \tau$, and letting $P_{l-1}(z) := P^{\dagger}_{l-1}(z)/(z-\tau)$, we get

$$A(z^d)B_l(z)P_{l-1}(z) = A(z)B_l(z^d)Q(z)\frac{\prod_{\gamma\in N_{l-1}(\tau)}(z^d-\gamma)}{z-\tau}. \tag{4.11}$$

Define

$$N_l(\tau) := \{\gamma \in N_{l-1}^{1/d}(\tau) \setminus \{\tau\} \mid B_l(\gamma) = 0\},$$
$$M_l(\tau) := \{\gamma \in N_{l-1}^{1/d}(\tau) \setminus \{\tau\} \mid B_l(\gamma) \neq 0\} \cup \{\tau\}.$$

If $\gamma \in N_{l-1}^{1/d}(\tau) \setminus \{\tau\}$, then $A(\gamma^d) \neq 0$ by (4.7) with $i = l-1$. Substituting $z = \gamma$ into (4.11), we get $B_l(\gamma)P_{l-1}(\gamma) = 0$. Hence, setting

$$B_{l+1}(z) := \frac{B_l(z)}{\prod_{\gamma\in N_l(\tau)}(z-\gamma)} \in \mathbb{C}[z], \quad P_l(z) := \frac{P_{l-1}(z)}{\prod_{\gamma\in M_l(\tau)\setminus\{\tau\}}(z-\gamma)} \in \mathbb{C}[z]$$

and dividing both sides of (4.11) by

$$\prod_{\gamma\in N_l(\tau)}(z-\gamma)\prod_{\gamma\in M_l(\tau)\setminus\{\tau\}}(z-\gamma) = \frac{\prod_{\gamma\in N_{l-1}(\tau)}(z^d-\gamma)}{z-\tau},$$

we obtain

$$A(z^d)B_{l+1}(z)P_l(z) = A(z)B_{l+1}(z^d)Q(z)\prod_{\gamma\in N_l(\tau)}(z^d-\gamma). \tag{4.12}$$

Since $\tau \in N_{l-1}^{1/d}(\tau)$ by (4.10), if $N_l(\tau) = \emptyset$, then $N_{l-1}^{1/d}(\tau) = M_l(\tau)$, and hence $M_l(\tau) = \zeta_d M_l(\tau)$. Then we let $k = l$, which implies the lemma because

$$P_l(z) = \frac{(z-\tau)P(z)}{\prod_{i=1}^{l}\prod_{\gamma\in M_i(\tau)}(z-\gamma)} \in \mathbb{C}[z].$$

If $N_l(\tau) \neq \emptyset$, for i ($\ge l+1$), we define inductively

$$N_i(\tau) := \{\gamma \in N_{i-1}^{1/d}(\tau) \mid B_i(\gamma) = 0\},$$
$$M_i(\tau) := \{\gamma \in N_{i-1}^{1/d}(\tau) \mid B_i(\gamma) \neq 0\},$$

and

$$B_{i+1}(z) := \frac{B_i(z)}{\prod_{\gamma\in N_i(\tau)}(z-\gamma)}, \quad P_i(z) := \frac{P_{i-1}(z)}{\prod_{\gamma\in M_i(\tau)}(z-\gamma)}$$

unless $N_{i-1}(\tau)$ is empty. Note that $B_{i+1}(z), P_i(z) \in \mathbb{C}[z]$, since for any γ in $N_{i-1}^{1/d}(\tau)$ we have $B_i(\gamma)P_{i-1}(\gamma) = 0$ by (4.12) and $A(\gamma^d) \neq 0$. In the same way as above, we have

$$A(z^d)B_{l+2}(z)P_{l+1}(z) = A(z)B_{l+2}(z^d)Q(z)\prod_{\gamma\in N_{l+1}(\tau)}(z^d-\gamma).$$

We repeat this process, which terminates in a finite number of steps since $B(z)$ is a polynomial. Thus there exists an integer $k \geq l$ such that

$$A(z^d)B_{k+1}(z)P_k(z) = A(z)B_{k+1}(z^d)Q(z)$$

and $N_k(\tau) = \emptyset$, which implies $N_{k-1}^{1/d}(\tau) = M_k(\tau)$, and hence $M_k(\tau) = \zeta_d M_k(\tau)$. ∎

Remark 4.3. The case where $\tau = -1$ and d is even corresponds to Lemma 4.1. The cases where $\tau = -1$ and d is odd and where $\tau = 1$ correspond to Lemma 4.2. We also note that the case where $-1 \in \tilde{\mathcal{F}}_k(\tau)$ occurs when d is even and $\tau = \pm 1$.

Let $H^{(\tau)}(z)$ be a polynomial defined by

$$H^{(\tau)}(z) = \prod_{\gamma \in N_{k-1}(\tau)} (z-\gamma) \cdots \prod_{\gamma \in N_0(\tau)} (z-\gamma),$$

where $N_i(\tau)$ $(0 \leq i \leq k-1)$ are defined in the proof of either Lemma 4.1 or 4.2.

Lemma 4.4. *The polynomial $B(z)$ is divisible by $H^{(\tau)}(z)$, and by factoring out we have an equation of the same form as* (2.7), *namely,*

$$A(z^d)B^\dagger(z)P^\dagger(z) = A(z)B^\dagger(z^d)Q^\dagger(z),$$

where

$$P^\dagger(z) = \frac{P(z)}{F^{(\tau)}(z)}, \qquad Q^\dagger(z) = \frac{Q(z)}{z-\tau}, \qquad B^\dagger(z) = \frac{B(z)}{H^{(\tau)}(z)}$$

if $\tau \notin \tilde{\mathcal{E}}_k(\tau)$, and

$$P^\dagger(z) = \frac{P(z)}{F^{(\tau)}(z)/(z-\tau)}, \qquad Q^\dagger(z) = Q(z), \qquad B^\dagger(z) = \frac{B(z)}{H^{(\tau)}(z)}$$

if $\tau \in \tilde{\mathcal{E}}_k(\tau)$.

Proof. The fact that $B(z)$ is divisible by $H^{(\tau)}(z)$ is shown in the proof of Lemma 4.1 or 4.2. By the definition of the sets therein, we have

$$(4.13)\quad \begin{aligned} &F^{(\tau)}(z)\\ &= \prod_{\gamma \in M_k(\tau)} (z-\gamma) \prod_{\gamma \in M_{k-1}(\tau)} (z-\gamma) \cdots \prod_{\gamma \in M_1(\tau)} (z-\gamma)\\ &= \prod_{\gamma \in N_{k-1}(\tau)} (z^d-\gamma) \prod_{\gamma \in N_{k-2}^{1/d}(\tau)\setminus N_{k-1}(\tau)} (z-\gamma) \cdots \prod_{\gamma \in N_0^{1/d}(\tau)\setminus N_1(\tau)} (z-\gamma) \end{aligned}$$

$$= \prod_{\gamma \in N_{k-1}(\tau)} \frac{z^d - \gamma}{z - \gamma} \prod_{\gamma \in N_{k-2}(\tau)} (z^d - \gamma)$$
$$\times \prod_{\gamma \in N_{k-3}^{1/d}(\tau) \setminus N_{k-2}(\tau)} (z - \gamma) \cdots \prod_{\gamma \in N_0^{1/d}(\tau) \setminus N_1(\tau)} (z - \gamma)$$
$$= \prod_{\gamma \in N_{k-1}(\tau)} \frac{z^d - \gamma}{z - \gamma} \prod_{\gamma \in N_{k-2}(\tau)} \frac{z^d - \gamma}{z - \gamma} \cdots \prod_{\gamma \in N_0(\tau)} \frac{z^d - \gamma}{z - \gamma} \prod_{\gamma \in N_0(\tau)} (z - \gamma)$$
$$= \frac{H^{(\tau)}(z^d)}{H^{(\tau)}(z)} (z - \tau).$$

Hence the lemma is proved by dividing both sides of (2.7) by $H^{(\tau)}(z)F^{(\tau)}(z) = H^{(\tau)}(z^d)(z-\tau)$ in the case of Lemma 4.1 and by $H^{(\tau)}(z)F^{(\tau)}(z)/(z-\tau) = H^{(\tau)}(z^d)$ in the case of Lemma 4.2. ∎

5. Proof of the theorems

Lemma 5.1 (A special case in Nishioka [4, Lemma 2.3.3]). *Let* $\boldsymbol{L}$ *be a subfield of* $\mathbb{C}$ *and suppose that*

$$f(z) \in \mathbb{C}[[z]] \cap \boldsymbol{L}(z).$$

If $f(z)$ *converges at* $z = \alpha$, *then* $f(\alpha) \in \boldsymbol{L}(\alpha)$.

Proof of Theorem 1.3. First we check the necessary conditions for algebraic dependence. Assume that the values $\Phi_1(\alpha^{-d^N}), \ldots, \Phi_m(\alpha^{-d^N})$ in Section 2 are algebraically dependent. As is mentioned in that section, there exist integers $e \geq 0$ and $e_i \geq 1$ $(1 \leq i \leq l)$, and coprime polynomials $A(z), B(z) \in \boldsymbol{K}[z] \setminus \{0\}$ satisfying the functional equation (2.6) with $b = 1$ by Lemma 3.2. Recall that $P_i(z) = 1 + p_i z + z^2$. We define

$$P(z) := \prod_{i=1}^{k} P_i(z)^{e_i} \quad \text{and} \quad Q(z) := (1 + z^2)^e \prod_{i=k+1}^{l} P_i(z)^{e_i},$$

and so $\deg P(z) = \deg Q(z)$. If $\gamma \in \mathbb{C}$ is a zero of $P(z)Q(z)$, then $\gamma = \pm\sqrt{-1}$ or $-(\gamma + \overline{\gamma}) \in \{a_1, \ldots, a_m\}$ by (2.3).

First we consider the case of $d = 2$. If $P(z)$ or $Q(z)$ has a real root, we take a real root α_1 of $P(z)Q(z)$ with the largest absolute value among its real roots, that is, α_1 satisfies (3.2). Exchanging the above definition of $P(z)$ and $Q(z)$ if necessary, we may assume that $P(\alpha_1) = 0$. If α_1 is positive, then case (i) of Theorem 1.3 holds by Lemma 3.4 and Remark 3.5. If α_1 is negative, then we have $\alpha_1 = -1$ by Lemma 3.3, namely, $P(-1) = 0$. Thus we see that $a_i = 2$ for some i, and case (ii) of Theorem 1.3 holds (see Remark 1.4).

Next we suppose that $P(z)Q(z)$ has non-real roots, which are included in the set $\mathcal{M}$ defined by (3.5) as is shown in Subsection 3.2. Exchanging the above definitions of $P(z)$ and $Q(z)$ if necessary, we may assume that $P(z)$ has a non-real root with the smallest positive argument among the roots of $P(z)Q(z)$ in $\mathcal{M}$. Then the assumptions of either Lemma 4.1 or Lemma 4.2 are satisfied. Setting $\mathcal{E}_k(\tau) := \tilde{\mathcal{E}}_k(\tau) \cup \overline{\tilde{\mathcal{E}}_k(\tau)}$, we have

$$\mathcal{E}_k(\tau) = \Gamma_1(\tau) \cup \cdots \cup \Gamma_{k-1}(\tau) \cup S_k(\tau),$$

where $S_k(\tau) = M_k(\tau) \cup \overline{M_k(\tau)}$, $\Lambda_i(\tau) = N_i(\tau) \cup \overline{N_i(\tau)}$ $(0 \le i \le k-1)$, and $\Gamma_i(\tau) = M_i(\tau) \cup \overline{M_i(\tau)}$ $(1 \le i \le k-1)$. Using the conditions on $M_i(\tau)$ $(1 \le i \le k)$, we see that the assumptions on $\mathcal{E}_k(\tau)$ stated in the Introduction are satisfied. Now we show that the set of roots of $P(z)Q(z)$ contains $\mathcal{F}_k(\tau)$. Note that if $\gamma \in \mathbb{C}$ is a zero of $P(z)$ (resp. $Q(z)$), then $\overline{\gamma}$ is also a zero of $P(z)$ (resp. $Q(z)$). If the assumptions of Lemma 4.1 are satisfied, then the set of roots of $P(z)$ (resp. $Q(z)$) contains $\mathcal{E}_k(\tau)$ (resp. $\{\tau, \overline{\tau}\}$). Since $P(z)$ and $Q(z)$ are coprime, $\tau \notin \mathcal{E}_k(\tau)$, and so $\mathcal{F}_k(\tau) = \mathcal{E}_k(\tau) \cup \{\tau, \overline{\tau}\}$. Thus the set of the roots of $P(z)Q(z)$ contains $\mathcal{F}_k(\tau)$ in this case. On the other hand, if the assumptions of Lemma 4.2 are satisfied, then we get $\mathcal{E}_k(\tau) \supset \{\tau, \overline{\tau}\}$ and $\mathcal{F}_k(\tau) = \mathcal{E}_k(\tau) \setminus \{\tau, \overline{\tau}\}$. Moreover, the set of the roots of $P(z)$ contains $\mathcal{F}_k(\tau)$. Hence case (ii) of Theorem 1.3 holds in both cases.

We now consider the case of $d \ge 3$. By (2.3) and Lemma 3.2, we get $b = 1$, and so d is even. By Lemma 3.6, the roots of $P(z)Q(z)$ are included in $\mathcal{M}$. By Lemma 4.1 or 4.2, there exist $\tau_1 \in \mathbb{C}$ with $|\tau_1| = 1$ and $\tilde{\mathcal{E}}_{k_1}(\tau_1)$ with $k_1 \ge 1$ such that

(i) $\tau_1 \notin \tilde{\mathcal{E}}_{k_1}(\tau_1)$ and $P(z), Q(z)$ are divisible by $F^{(\tau_1)}(z), z - \tau_1$, respectively, or
(ii) $\tau_1 \in \tilde{\mathcal{E}}_{k_1}(\tau_1)$ and $P(z)$ is divisible by $F^{(\tau_1)}(z)/(z - \tau_1)$.

Dividing (2.7) by these terms, from Lemma 4.4 we have

$$A(z^d)B^\dagger(z)P^\dagger(z) = A(z)B^\dagger(z^d)Q^\dagger(z),$$

which has the same form as (2.7). For convenience, denote $\eta^{(1)}(z) := P^\dagger(z)$ and $\xi^{(1)}(z) := Q^\dagger(z)$. Since the number of the elements in $\tilde{\mathcal{E}}_{k_1}(\tau_1)$ is not less than $d > 2$, we have $\deg \eta^{(1)}(z) < \deg \xi^{(1)}(z)$. In particular, $\deg \eta^{(1)}(z)\xi^{(1)}(z) > 0$. Let $\alpha^{(1)} \in \mathbb{C}$ with $|\alpha^{(1)}| = 1$ be a root of $\eta^{(1)}(z)\xi^{(1)}(z)$ having the smallest positive argument among its roots. If $\xi^{(1)}(\alpha^{(1)}) \neq 0$, then $\eta^{(1)}(\alpha^{(1)}) = 0$. We apply Lemma 4.4 with $P(z) = \eta^{(1)}(z)$ and $Q(z) = \xi^{(1)}(z)$. We write the polynomials corresponding to $P^\dagger(z)$ and $Q^\dagger(z)$ therein as $\eta^{(2)}(z)$ and $\xi^{(2)}(z)$, respectively. Then we see that $\deg \eta^{(2)}(z) < \deg \xi^{(2)}(z)$. Repeating this process, we can define $\eta^{(i)}(z), \xi^{(i)}(z)$, and $\alpha^{(i)}$ $(i = 2, 3, \ldots)$ inductively whenever $\xi^{(i-1)}(\alpha^{(i-1)}) \neq 0$. This process terminates in a finite number of steps since $P^\dagger(z)$ is a polynomial.

Thus there exists an integer $k \ge 1$ such that $\xi^{(k)}(\alpha^{(k)}) = 0$. Since $\eta^{(k)}(z)$ and $\xi^{(k)}(z)$ are factors of $P^\dagger(z)$ and $Q^\dagger(z)$, respectively, Lemma 4.1 or 4.2

implies the following: There exist $\tau_2 \in \mathbb{C}$ with $|\tau_2| = 1$ and $\tilde{\mathcal{E}}_{k_2}(\tau_2)$ with $k_2 \geq 1$ such that

(i) $\tau_2 \notin \tilde{\mathcal{E}}_{k_2}(\tau_2)$ and $Q^\dagger(z), P^\dagger(z)$ are divisible by $F^{(\tau_2)}(z), z - \tau_2$, respectively, or

(ii) $\tau_2 \in \tilde{\mathcal{E}}_{k_2}(\tau_2)$ and $Q^\dagger(z)$ is divisible by $F^{(\tau_2)}(z)/(z - \tau_2)$.

We note that $\tau_1 \neq \tau_2$, since $B(\tau_1) = A(\tau_2) = 0$ and since $A(z)$ and $B(z)$ are coprime. For $j = 1, 2$, we set $\mathcal{E}_{k_j}(\tau_j) := \tilde{\mathcal{E}}_{k_j}(\tau_j) \cup \overline{\tilde{\mathcal{E}}_{k_j}(\tau_j)}$. As in the case where $d = 2$ and $P(z)Q(z)$ has non-real roots, we see that the set of roots of $P(z)$ (resp. $Q(z)$) contains $\mathcal{E}_{k_1}(\tau_1) \setminus \{\tau_1, \overline{\tau_1}\}$ (resp. $\mathcal{E}_{k_2}(\tau_2) \setminus \{\tau_2, \overline{\tau_2}\}$) both in the case of Lemmas 4.1 and 4.2. Since $P(z)$ and $Q(z)$ are coprime, we obtain

$$(\mathcal{E}_{k_1}(\tau_1) \setminus \{\tau_1, \overline{\tau_1}\}) \cap (\mathcal{E}_{k_2}(\tau_2) \setminus \{\tau_2, \overline{\tau_2}\}) = \emptyset,$$

and so

$$\mathcal{F}_{k_1}(\tau_1) \cap \mathcal{F}_{k_2}(\tau_2) \subset (\mathcal{E}_{k_1}(\tau_1) \cap \mathcal{E}_{k_2}(\tau_2)) \cup \{\tau_1, \overline{\tau_1}, \tau_2, \overline{\tau_2}\} \subset \{\tau_1, \overline{\tau_1}, \tau_2, \overline{\tau_2}\}.$$

Hence we obtain case (iii) of Theorem 1.3.

In what follows, we show that $\Phi_1(\alpha^{-d^N}), \ldots, \Phi_m(\alpha^{-d^N})$ are algebraically dependent under the assumption that case (i), (ii), or (iii) in Theorem 1.3 holds. Recall by (2.3) that $p_i = a_i$ $(i = 1, \ldots, m)$ and $b = 1$ since d is even in every case. It suffices to show that there exist a non-empty subset I of $\{1, \ldots, m\}$ and non-zero integers e_i $(i \in I)$ satisfying

$$\prod_{i \in I} c_i(z)^{e_i} = \prod_{i \in I} \left(\frac{z^2 + 1}{z^2 + a_i z + 1} \right)^{e_i} \in H_d, \tag{5.1}$$

where H_d is the subgroup of the multiplicative group $\boldsymbol{K}(z)^\times$ defined by (2.1), or there exists a $g(z) \in \boldsymbol{K}(z)^\times$ such that

$$\prod_{i \in I} c_i(z)^{e_i} = \frac{g(z^d)}{g(z)}.$$

Here, if $z = 0$ is a zero or a pole of $g(z)$, then it is a zero or a pole of $g(z^d)/g(z)$, respectively. Hence $g(0) \neq 0$ because $c_i(0) = 1$ $(i \in I)$. Then we see by (2.5) that $F(z) := g(z)^{-1} \prod_{i \in I} \Phi_i(z)^{e_i} \in \boldsymbol{K}[[z]]$ satisfies $F(z^d) = F(z)$, which holds only if $F(z) = \lambda \in \boldsymbol{K}$. In fact, if l (≥ 1) is the lowest degree of non-constant terms of $F(z)$, then that of $F(z^d)$ is dl, which contradicts $F(z^d) = F(z)$. Hence

$$\prod_{i \in I} \Phi_i(z)^{e_i} = \lambda g(z) \in \boldsymbol{K}[[z]] \cap \boldsymbol{K}(z).$$

By Lemma 5.1 we have

$$\prod_{i \in I} \Phi_i(\alpha^{-d^N})^{e_i} \in \boldsymbol{K},$$

which implies that $\Phi_1(\alpha^{-d^N}),\dots,\Phi_m(\alpha^{-d^N})$ are algebraically dependent and thus we have only to prove (5.1).

Note that, for any $h\ge 1$ and $g(z)\in \boldsymbol{K}(z)^\times$,

$$\frac{g(z^{d^h})}{g(z)}=\frac{g(z^d)}{g(z)}\frac{g(z^{d^2})}{g(z^d)}\cdots\frac{g(z^{d^h})}{g(z^{d^{h-1}})}\in H_d. \tag{5.2}$$

If $d=2$, then for the proof of (5.1) it suffices to check that

$$\prod_{i\in I}(z^2+a_iz+1)^{e_i}\in H_2 \tag{5.3}$$

because

$$z^2+1=\frac{z^4-1}{z^2-1}\in H_2. \tag{5.4}$$

First we suppose that case (i) of Theorem 1.3 holds. Since $b_1=-b_2$, we have

$$(z^2+b_1z+1)(z^2+b_2z+1)=z^4-(b_2^2-2)z^2+1,$$

and then

$$(z^2+b_1z+1)(z^2+b_2z+1)\prod_{j=3}^{l-1}(z^{2^{j-1}}+b_jz^{2^{j-2}}+1)=z^{2^{l-1}}+b_lz^{2^{l-2}}+1 \tag{5.5}$$

by $b_j=b_{j-1}^2-2$ $(j=3,\dots,l-1)$ and $b_l=-b_{l-1}^2+2$. Therefore by (5.2) and (5.5) we obtain

$$\begin{aligned}(z^2+b_lz+1)^{-1}&\prod_{j=1}^{l-1}(z^2+b_jz+1)\\ &=\frac{z^{2^{l-1}}+b_lz^{2^{l-2}}+1}{z^2+b_lz+1}\prod_{j=3}^{l-1}\left(\frac{z^2+b_jz+1}{z^{2^{j-1}}+b_jz^{2^{j-2}}+1}\right)\in H_2,\end{aligned}$$

which implies (5.3).

Here we suspend the proof of the theorem and investigate the properties of the sets defined in Section 1. For convenience, denote $\Gamma_k(\tau):=S_k(\tau)$. Then $\mathcal{E}_k(\tau)=\bigcup_{i=1}^k\Gamma_i(\tau)$.

Lemma 5.2. *Let $\tau\in\mathbb{C}$ with $|\tau|=1$, $k\ge1$, and $S_k(\tau)\subset\Omega_k(\tau)$ satisfy* (1.4). *Suppose that $\tau\in\mathcal{E}_k(\tau)$. Then*

$$\mathrm{Card}\{i\mid 1\le i\le k,\ \tau\in\Gamma_i(\tau)\}=\mathrm{Card}\{i\mid 1\le i\le k,\ \overline{\tau}\in\Gamma_i(\tau)\}=1,$$

where Card *denotes cardinality.*

Proof. Since $\overline{\Gamma_i(\tau)}=\Gamma_i(\tau)$ for $i=1,\dots,k$, it suffices to show that

$$\mathrm{Card}\{i\mid 1\le i\le k,\ \tau\in\Gamma_i(\tau)\}=1. \tag{5.6}$$

For $x,y\in\mathbb{C}$, we write $x\sim y$ if $x=y$ or if $\overline{x}=y$. Noting that $\tau\in\mathcal{E}_k(\tau)\subset\bigcup_{i=1}^k\Omega_i(\tau)$, we take $l:=\min\{i\ge1\mid \tau^{d^i}\sim\tau\}$ $(\le k)$. Suppose that $\tau\in\Gamma_j(\tau)\subset\Omega_j(\tau)$ for some $j\ge1$. Set $j=ql+r$, where q and r are integers with $q \geq 0$ and $0 \leq r \leq l-1$. Then $\tau \sim \tau^{d^j} = \tau^{d^{ql+r}} \sim \tau^{d^r}$, and so $r = 0$ by the minimality of l. We take $b := \min\{q \geq 1 \mid \tau \in \Gamma_{ql}(\tau)\}$. For the proof of (5.6), it suffices to show that $\tau \notin \Gamma_{bl+cl}(\tau)$ for any $c \geq 1$.

Suppose on the contrary that $\tau \in \Gamma_{bl+cl}(\tau)$. Then $\tau^d \in \Lambda_{bl+cl-1}(\tau)$. Note that for any i, j with $i \geq j$, if $\gamma \in \Lambda_i(\tau)$, then $\gamma^{d^{i-j}} \in \Lambda_j(\tau)$. Thus $\tau \sim \tau^{d^{cl}} = (\tau^d)^{d^{cl-1}} \in \Lambda_{bl}(\tau)$. Since $\overline{\Lambda_{bl}(\tau)} = \Lambda_{bl}(\tau)$, we obtain $\tau \in \Lambda_{bl}(\tau)$, which contradicts the fact that $\Gamma_{bl}(\tau) \cap \Lambda_{bl}(\tau) = \emptyset$. ∎

Define

$$g_\gamma(z) = (z-\gamma)(z-\overline{\gamma}) \tag{5.7}$$

for $\gamma \in \mathbb{C}$.

LEMMA 5.3. *Let $\tau \in \mathbb{C}$ with $|\tau| = 1$, $k \geq 1$, and $S_k(\tau) \subset \Omega_k(\tau)$ satisfy* (1.4). *Then there exists an integer valued function e on $\mathcal{F}_k(\tau)$ such that*

$$e(\gamma) = e(\overline{\gamma}) \neq 0 \tag{5.8}$$

for any $\gamma \in \mathcal{F}_k(\tau)$ and

$$\prod_{\gamma \in \mathcal{F}_k(\tau)} g_\gamma(z)^{e(\gamma)} \in H_d, \tag{5.9}$$

where H_d is the subgroup of $\boldsymbol{K}(z)^\times$ defined by (2.1). *In particular, there exists an integer p such that*

$$(z^2+1)^p \prod_{\gamma \in \mathcal{F}_k(\tau) \setminus \{\pm\sqrt{-1}\}} g_\gamma(z)^{e(\gamma)} \in H_d. \tag{5.10}$$

Proof. It suffices to show (5.9) because $g_{\sqrt{-1}}(z) = g_{-\sqrt{-1}}(z) = z^2+1$. Set $\Lambda_i^{1/d}(\tau) = \{\gamma \in \mathbb{C} \mid \gamma^d \in \Lambda_i(\tau)\}$ for $i = 0, 1, \ldots, k-2$ and

$$g(\mathcal{E}_k(\tau); z) = \prod_{\gamma \in S_k(\tau)} g_\gamma(z) \prod_{\gamma \in \Gamma_{k-1}(\tau)} g_\gamma(z) \cdots \prod_{\gamma \in \Gamma_1(\tau)} g_\gamma(z).$$

In the same way as for (4.13), noting that $S_k(\tau) = \Lambda_{k-1}^{1/d}(\tau)$ by $S_k(\tau) = M_k(\tau) \cup \overline{M_k(\tau)}$, $M_k(\tau) = N_{k-1}^{1/d}(\tau)$, and $\Lambda_{k-1}(\tau) = N_{k-1}(\tau) \cup \overline{N_{k-1}(\tau)}$, we see that

$$\begin{aligned} g(\mathcal{E}_k(\tau); z) &= \prod_{\gamma \in \Lambda_{k-1}(\tau)} g_\gamma(z^d) \prod_{\gamma \in \Lambda_{k-2}^{1/d}(\tau) \setminus \Lambda_{k-1}(\tau)} g_\gamma(z) \cdots \prod_{\gamma \in \Lambda_0^{1/d}(\tau) \setminus \Lambda_1(\tau)} g_\gamma(z) \\ &= \prod_{\gamma \in \Lambda_{k-1}(\tau)} \frac{g_\gamma(z^d)}{g_\gamma(z)} \prod_{\gamma \in \Lambda_{k-2}(\tau)} g_\gamma(z^d) \\ &\quad \times \prod_{\gamma \in \Lambda_{k-3}^{1/d}(\tau) \setminus \Lambda_{k-2}(\tau)} g_\gamma(z) \cdots \prod_{\gamma \in \Lambda_0^{1/d}(\tau) \setminus \Lambda_1(\tau)} g_\gamma(z) \end{aligned}$$

$$= \prod_{\gamma\in\Lambda_{k-1}(\tau)} \frac{g_\gamma(z^d)}{g_\gamma(z)} \prod_{\gamma\in\Lambda_{k-2}(\tau)} \frac{g_\gamma(z^d)}{g_\gamma(z)} \cdots \prod_{\gamma\in\Lambda_0(\tau)} \frac{g_\gamma(z^d)}{g_\gamma(z)} \prod_{\gamma\in\Lambda_0(\tau)} g_\gamma(z).$$

Since $\Lambda_0(\tau) = \{\tau, \overline{\tau}\}$, we obtain

$$g^*(z) := g(\mathcal{E}_k(\tau); z) \prod_{\gamma\in\{\tau,\overline{\tau}\}} g_\gamma(z)^{-1} \in H_d. \tag{5.11}$$

Note that for $\gamma \in \mathbb{C}$,

$$\gamma \in \mathcal{E}_k(\tau) \quad \text{if and only if} \quad g(\mathcal{E}_k(\tau); \gamma) = 0. \tag{5.12}$$

Suppose first that $\tau \notin \mathcal{E}_k(\tau)$. Then (5.7) and (5.11) imply (5.8) and (5.9) because $\mathcal{F}_k(\tau) = \mathcal{E}_k(\tau) \cup \{\tau, \overline{\tau}\}$. Noting that $\overline{\tau} \notin \mathcal{E}_k(\tau)$ by $\overline{\mathcal{E}_k(\tau)} = \mathcal{E}_k(\tau)$, we get $e(\gamma) \neq 0$ for any $\gamma \in \mathcal{F}_k(\tau)$ by (5.12). Next assume that $\tau \in \mathcal{E}_k(\tau)$. Then Lemma 5.2 implies that $g^*(z)$ is a polynomial with $g^*(\tau) \neq 0$ and $g^*(\overline{\tau}) \neq 0$. Thus (5.7) and (5.11) imply (5.8) and (5.9) by $\mathcal{F}_k(\tau) = \mathcal{E}_k(\tau) \setminus \{\tau, \overline{\tau}\}$. Moreover, $e(\gamma) \neq 0$ for any $\gamma \in \mathcal{F}_k(\tau)$ by (5.12). ∎

Continuation of the proof of Theorem 1.3. Suppose that case (ii) of Theorem 1.3 holds. Then for any $\gamma \in \mathcal{F}_k(\tau) \setminus \{\pm\sqrt{-1}\}$ we have $a_{i(\gamma)} = -(\gamma + \overline{\gamma})$ for some $1 \le i(\gamma) \le m$. Using (5.4) and (5.10), we obtain

$$\prod_{\gamma\in\mathcal{F}_k(\tau)\setminus\{\pm\sqrt{-1}\}} (z^2 + a_{i(\gamma)}z + 1)^{e(\gamma)} \in H_2, \qquad e(\gamma) \neq 0,$$

which implies (5.3) with a non-empty subset I of $\{1, \ldots, m\}$ and integers e_i ($i \in I$). Note that for $\gamma, \eta \in \mathcal{F}_k(\tau) \setminus \{\pm\sqrt{-1}\}$, $a_{i(\gamma)} = a_{i(\eta)}$ if and only if $\gamma \sim \eta$. Moreover, if $\gamma \sim \eta$, then $e(\gamma) = e(\eta)$ by (5.8). Hence $e_i \neq 0$ for any $i \in I$.

Next suppose that case (iii) of Theorem 1.3 holds. Then, for any $\gamma \in \mathcal{F}_{k_1}(\tau_1) \setminus \{\pm\sqrt{-1}\}$ (resp. $\gamma \in \mathcal{F}_{k_2}(\tau_2) \setminus \{\pm\sqrt{-1}\}$), we have $a_{i(\gamma)} = -(\gamma + \overline{\gamma})$ for some $i(\gamma)$ (resp. $a_{j(\gamma)} = -(\gamma + \overline{\gamma})$ for some $j(\gamma)$). Combining (2.5) and (5.10), we get

$$(z^2+1)^{q_1} \prod_{\gamma\in\mathcal{F}_{k_1}(\tau_1)\setminus\{\pm\sqrt{-1}\}} c_{i(\gamma)}(z)^{e(\gamma)} \in H_d,$$

$$(z^2+1)^{q_2} \prod_{\gamma\in\mathcal{F}_{k_2}(\tau_2)\setminus\{\pm\sqrt{-1}\}} c_{j(\gamma)}(z)^{e'(\gamma)} \in H_d,$$

where q_1, q_2, $e(\gamma) = e(\mathcal{F}_{k_1}(\tau_1); \gamma)$, and $e'(\gamma) = e(\mathcal{F}_{k_2}(\tau_2); \gamma)$ are integers with $e(\gamma)$, $e'(\gamma) \neq 0$.

We show that (5.1) is satisfied with a non-empty subset I of $\{1, \ldots, m\}$ and integers e_i ($i \in I$). The case where $q_1 = 0$ or $q_2 = 0$ is clear. If $q_1 \neq 0$

and $q_2 \neq 0$, then (5.1) follows from

$$\prod_{\gamma\in\mathcal{F}_{k_1}(\tau_1)\setminus\{\pm\sqrt{-1}\}} c_{i(\gamma)}(z)^{-q_2e(\gamma)} \prod_{\gamma\in\mathcal{F}_{k_2}(\tau_2)\setminus\{\pm\sqrt{-1}\}} c_{j(\gamma)}(z)^{q_1e'(\gamma)} \in H_d.$$

By (5.8), to prove the existence of the subset I such that $e_i \neq 0$ $(i \in I)$, we have only to show that

$$\mathcal{F}_{k_1}(\tau_1) \setminus \{\pm\sqrt{-1}\} \neq \mathcal{F}_{k_2}(\tau_2) \setminus \{\pm\sqrt{-1}\}. \tag{5.13}$$

Suppose on the contrary that

$$\mathcal{F}_{k_1}(\tau_1) \setminus \{\pm\sqrt{-1}\} = \mathcal{F}_{k_2}(\tau_2) \setminus \{\pm\sqrt{-1}\}. \tag{5.14}$$

Then, using (5.14) and the assumptions on $\mathcal{F}_{k_i}(\tau_i)$ for $i = 1, 2$, we get

(5.15)

$$\begin{aligned}\mathcal{E}_{k_i}(\tau_i) \subset \mathcal{F}_{k_i}(\tau_i) \cup \{\tau_i, \overline{\tau_i}\} &\subset (\mathcal{F}_{k_1}(\tau_1) \cap \mathcal{F}_{k_2}(\tau_2)) \cup \{\tau_i, \overline{\tau_i}, \sqrt{-1}, -\sqrt{-1}\}\\ &\subset \{\tau_1, \overline{\tau_1}, \tau_2, \overline{\tau_2}, \sqrt{-1}, -\sqrt{-1}\}.\end{aligned}$$

If there exists an $i \in \{1, 2\}$ such that $\tau_i \notin \mathbb{R}$, then $\mathcal{E}_{k_i}(\tau_i)$ contains at least $2d \geq 8$ elements by (1.4). This contradicts (5.15). Hence we see that $\tau_1, \tau_2 \in \{1, -1\}$ by $|\tau_1| = |\tau_2| = 1$, and so $\tau_h = -1$ for some $h \in \{1, 2\}$ by $\tau_1 \neq \tau_2$. Therefore $\mathcal{E}_{k_h}(-1) \subset \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$ by (5.15). Since $\mathcal{E}_{k_h}(-1)$ contains at least $d \geq 4$ elements by (1.4), we obtain $\mathcal{E}_{k_h}(-1) = \{1, -1, \sqrt{-1}, -\sqrt{-1}\}$, which is impossible because $1 \notin \Omega_i(-1)$ for any $i \geq 1$. This completes the proof of Theorem 1.3. ∎

Proof of Theorem 1.1. If the values $\Phi_1(\alpha^{-d^N}), \ldots, \Phi_m(\alpha^{-d^N})$ in Section 2 are algebraically dependent, then we see that $b = 1$ and d is odd by (2.3) and Lemma 3.2. The theorem can be proved in a similar way to Theorem 1.3 only except the following: We show that the sets $\mathcal{F}_{k_1}(\tau_1)$ and $\mathcal{F}_{k_2}(\tau_2)$ satisfy (5.13). Suppose on the contrary that (5.14) holds. Then, using the assumptions on $\mathcal{F}_{k_i}(\tau_i)$ for $i = 1, 2$, we get

(5.16)

$$\begin{aligned}S_{k_i}(\tau_i) \subset \mathcal{F}_{k_i}(\tau_i) \cup \{\tau_i, \overline{\tau_i}\} &\subset (\mathcal{F}_{k_1}(\tau_1) \cap \mathcal{F}_{k_2}(\tau_2)) \cup \{\tau_i, \overline{\tau_i}, \sqrt{-1}, -\sqrt{-1}\}\\ &\subset \{\tau_1, \overline{\tau_1}, \tau_2, \overline{\tau_2}, \sqrt{-1}, -\sqrt{-1}\}.\end{aligned}$$

If there exists an $i \in \{1, 2\}$ such that $\tau_i \notin \mathbb{R}$, then by the assumptions on $S_{k_i}(\tau_i)$ we see that $S_{k_i}(\tau_i)$ contains at least $2d$ elements. Thus (5.16) implies that $d = 3$ and

$$S_{k_i}(\tau_i) = \{\tau_1, \overline{\tau_1}, \tau_2, \overline{\tau_2}, \sqrt{-1}, -\sqrt{-1}\}.$$

Hence

$$\sqrt{-1}^{3^{k_i}} = \tau_i \quad \text{or} \quad \sqrt{-1}^{3^{k_i}} = \overline{\tau_i}.$$

Consequently, $\tau_i = \sqrt{-1}$ or $\tau_i = -\sqrt{-1}$, and so $6 \leq \operatorname{Card} S_k(\tau_i) \leq 4$ by (5.16), a contradiction.

We now assume that $\tau_1, \tau_2 \in \mathbb{R}$. Since $|\tau_1| = |\tau_2| = 1$, (5.16) implies that, for $i = 1, 2$,

$$S_{k_i}(\tau_i) \subset \{1, -1, \sqrt{-1}, -\sqrt{-1}\},$$

which contradicts the fact that $S_{k_i}(\tau_i) = \zeta_d S_{k_i}(\tau_i)$ since d is odd. This completes the proof of (5.13) and Theorem 1.1. ∎

Acknowledgements. The first author was supported by Grant-in-Aid for JSPS Fellows (grant number 11J00168).

References

[1] K. K. Kubota, *On the algebraic independence of holomorphic solutions of certain functional equations and their values*, Math. Ann. 227 (1977), 9–50.

[2] T. Kurosawa, Y. Tachiya, and T. Tanaka, *Algebraic independence of infinite products generated by Fibonacci numbers*, Tsukuba J. Math. 34 (2010), 255–264.

[3] T. Kurosawa, Y. Tachiya, and T. Tanaka, *Algebraic relations with the infinite products generated by Fibonacci numbers*, Ann. Math. Inform. 41 (2013), 107–119.

[4] K. Nishioka, *Mahler Functions and Transcendence*, Lecture Notes in Math. 1631, Springer, 1996.

[5] Y. Tachiya, *Transcendence of certain infinite products*, J. Number Theory 125 (2007), 182–200.

Hajime Kaneko
Institute of Mathematics
University of Tsukuba
1-1-1, Tennodai
Tsukuba, Ibaraki 350-0006, Japan
E-mail: kanekoha@math.tsukuba.ac.jp

Takeshi Kurosawa
Department of Mathematical Information Science
Tokyo University of Science
1-3, Kagurazaka, Shinjuku-ku
Tokyo 162–8601, Japan
E-mail: tkuro@rs.kagu.tus.ac.jp

Yohei Tachiya
Graduate School of Science and Technology
Hirosaki University
Hirosaki 036-8561, Japan
E-mail: tachiya@cc.hirosaki-u.ac.jp

Taka-aki Tanaka
Department of Mathematics
Keio University
3-14-1, Hiyoshi, Kohoku-ku
Yokohama 223-8522, Japan
E-mail: takaaki@math.keio.ac.jp

Received on 8.5.2014
and in revised form on 21.11.2014 (7801)