CARPATHIAN J. MATH. **34** (2018), No. 2, 157 - 166
Online version at http://carpathian.ubm.ro
Print Edition: ISSN 1584 - 2851 Online Edition: ISSN 1843 - 4401

On linear independence of trigonometric numbers

ARNO BERGER

ABSTRACT. A necessary and sufficient condition is established for 1, $\cos(\pi r_1)$, and $\cos(\pi r_2)$ to be rationally independent, where r_1, r_2 are rational numbers. The elementary computational argument yields linear independence over larger number fields as well.

1. INTRODUCTION

Denote the field of all rational numbers by $\mathbb{Q}$. For every $r \in \mathbb{Q}$ let $N(r)$ be the smallest positive integer for which $rN(r)$ is an integer, i.e., $N(r) = q$ if $r = p/q$ with coprime integers p and $q > 0$. Given $r \in \mathbb{Q}$, the algebraic properties of trigonometric numbers such as $\cos(\pi r)$, $\sin(\pi r)$, and $\tan(\pi r)$ have long been of interest; see, e.g., [11, 13, 15] for time-honoured, and [2, 7, 16] for more recent accounts. A classical fact in this regard, already recorded in [15] but sometimes attributed to [13] as *Niven's Theorem*, is

$$\{2\cos(\pi r) : r \in \mathbb{Q}\} \cap \mathbb{Q} = \{-2, -1, 0, 1, 2\}\,. \tag{1.1}$$

Analogous results exist for $\sin(\pi r)$ and $\tan(\pi r)$. This note is motivated by an equivalent form of (1.1), namely

Fact 1. *Let $r \in \mathbb{Q}$. Then the following are equivalent:*

(i) *The numbers 1 and $\cos(\pi r)$ are linearly independent over $\mathbb{Q}$;*
(ii) $N(r) \geq 4$.

Fact 1 naturally raises the question whether it extends in any recognizable form to more than one trigonometric number. While this question does not seem to have been studied directly, there is a sizeable literature on the related classical subject of vanishing sums of roots of unity; see, e.g., [3, 12, 10] and references therein. Utilizing the latter, it is not hard to deduce the main result of the present note, Theorem 1.1 below, from [3, Thm.7], for instance. This note, however, proves Theorem 1.1 in an entirely different way, following a simple computational approach that does not invoke advanced algebraic number theory. The ensuing result is a true analogue of Fact 1 for *two* trigonometric numbers $\cos(\pi r_1)$ and $\cos(\pi r_2)$. To see what such an analogue might look like, note that clearly those two numbers are rationally dependent whenever $r_1 - r_2$ or $r_1 + r_2$ is an integer. Moreover,

$$2\cos(\pi/5) - 2\cos(2\pi/5) = 1\,, \tag{1.2}$$

so $1, \cos(\pi r_1)$, and $\cos(\pi r_2)$ may be linearly dependent over $\mathbb{Q}$ if $N(r_1) = N(r_2) = 5$. As it turns out, there are no other obstacles to rational independence.

Theorem 1.1. *Let $r_1, r_2 \in \mathbb{Q}$ be such that neither $r_1 - r_2$ nor $r_1 + r_2$ is an integer. Then the following are equivalent:*

(i) *The numbers 1, $\cos(\pi r_1)$, and $\cos(\pi r_2)$ are linearly independent over $\mathbb{Q}$;*

Received: 28.04.2017. In revised form: 01.03.2018. Accepted: 08.03.2018
2010 *Mathematics Subject Classification.* 11R09, 11R11, 12Y05.
Key words and phrases. *Niven's Theorem, trigonometric number, rational (in)dependence, cyclotomic polynomial, real quadratic number field.*

(ii) $N(r_j) \geq 4$ *for* $j \in \{1,2\}$, *and* $\big(N(r_1), N(r_2)\big) \neq (5,5)$.

A proof of Theorem 1.1 is given in Section 3. There it will also be seen that the three numbers in (i) often are linearly independent over larger number fields. As the reader may suspect, the part of Theorem 1.1 most challenging to establish, by far, is that (ii)⇒(i). With all technical details deferred to subsequent sections, the strategy of this part of the proof actually is quite simple: On the one hand, if 1, $\cos(\pi r_1)$, and $\cos(\pi r_2)$ are rationally dependent then the coefficients of the minimal polynomials over $\mathbb{Q}$ of $\cos(\pi r_1)$ and $\cos(\pi r_2)$, respectively, entail certain algebraic identities. Validity of these identities, on the other hand, is contradictory, unless $\min_{j=1}^{2} N(r_j) \leq 3$ or $\big(N(r_1), N(r_2)\big) = (5,5)$. To get a very concrete foretaste of the nature of this argument, consider for example the trigonometric numbers $z_1 = 2\cos(\pi/7)$ and $z_2 = 2\cos(\pi/9)$, whose minimal polynomials over $\mathbb{Q}$ are

$$P_7(z) = z^3 - z^2 - 2z + 1 \quad \text{and} \quad P_9(z) = z^3 - 3z - 1\,,$$

respectively. Assume that

$$rz_1 + sz_2 + t = 0 \quad \text{for some } r,s,t \in \mathbb{Q}\,. \tag{1.3}$$

Since z_1, z_2 clearly are irrational, $t = 0$ whenever $rs = 0$. Thus suppose $rs \neq 0$, and w.l.o.g. let $r = -1$, i.e., $z_1 = sz_2 + t$. Then

$$0 = s^{-3}P_7(sz_2 + t) = z_2^3 + \frac{3t-1}{s}z_2^2 + \frac{3t^2 - 2t - 2}{s^2}z_2 + \frac{P_7(t)}{s^3}\,.$$

Since the (monic) minimal polynomial of z_2 is unique, it follows that

$$3t - 1 = 0\,, \quad 3t^2 - 2t - 2 = -3s^2\,, \quad P_7(t) = -s^3\,,$$

and hence $t = \frac{1}{3}$ and $s^2 = \frac{7}{9}$. The latter clearly contradicts $s \in \mathbb{Q}$. Thus (1.3) is possible only if $r = s = t = 0$. In other words, the numbers 1, $\cos(\pi/7)$, and $\cos(\pi/9)$ are linearly independent over $\mathbb{Q}$.

As evidenced by this simple example, the proof of Theorem 1.1 presented in this note crucially depends on certain basic properties of the minmal polynomial of $\cos(\pi r)$ which themselves follow quite directly from elementary facts about cyclotomic polynomials. For the reader's convenience, Section 2 recalls all required algebraic facts, or establishes them in cases where no reference is known to the author.

Remark 1.1. For simplicity, this note only considers numbers $\cos(\pi r)$ with $r \in \mathbb{Q}$. However, similar results hold for other trigonometric numbers. For instance, Fact 1 yields that 1 and $\sin(\pi r)$ are rationally independent precisely if $N(r) \notin \{1,2,6\}$; and Theorem 1.1 implies that for $r_1, r_2 \in \mathbb{Q}$ with neither $r_1 - r_2$ nor $r_1 + r_2$ being an integer, the numbers 1, $\sin(\pi r_1)$, and $\sin(\pi r_2)$ are linearly independent over $\mathbb{Q}$ if and only if $N(r_j) \notin \{1,2,6\}$ for $j \in \{1,2\}$, and $\big(N(r_1), N(r_2)\big) \neq (10,10)$.

2. Cyclotomic and other polynomials

Denote the sets of all positive integers and all integers by $\mathbb{N}$ and $\mathbb{Z}$, respectively. For every $n \in \mathbb{N}$ let $\Phi_n = \Phi_n(z)$ be the n-th cyclotomic polynomial,

$$\Phi_n(z) = \prod\nolimits_{1 \leq j \leq n:\gcd(j,n)=1} \left(z - e^{2\pi\imath j/n}\right)\,. \tag{2.1}$$

It is well known that each Φ_n is monic with integer coefficients, is irreducible over $\mathbb{Q}$, and has degree $\varphi(n)$, where φ denotes the Euler totient function. For $n \geq 2$ the polynomial Φ_n is also palindromic, i.e., $\Phi_n(z^{-1}) = z^{-\varphi(n)}\Phi_n(z)$. The coefficients of Φ_n are traditionally labelled $a(j,n)$, thus

$$\Phi_n(z) = \sum\nolimits_{j=0}^{\varphi(n)} a(j,n) z^{\varphi(n)-j}\,; \tag{2.2}$$

in addition, let $a(j,n) = 0$ whenever $j > \varphi(n)$, so that $a(j,n)$ is defined for all $n \in \mathbb{N}$ and $j \geq 0$. (For later convenience, the labelling in (2.2) is a reversal of the traditional one.) The integers $a(j,n)$ are objects of great combinatorial interest and have been studied extensively; e.g., see [1] and references therein. Only a few specific properties of Φ_n are needed in this note and will now be reviewed; for comprehensive accounts the reader is referred, e.g., to [6, Ch.V.8], [9, §13], or [14, §11].

First, observe that while the values of $|a(j,n)|$ may be large for large n and the appropriate j, the four leading coefficients of Φ_n only attain values in $\{-1,0,1\}$, and in fact exhibit patterns that are even more restricted. Recall that $k \in \mathbb{Z}$ is *squarefree* if $p^2 \nmid k$, i.e., k is not divisible by p^2, for any prime number p.

Lemma 2.1. *Assume that $n \in \mathbb{N}$ is squarefree. Then $a(0,n) = 1$, and the coefficient triple $\big(a(1,n), a(2,n), a(3,n)\big)$ has exactly one of the following eight values:*

$$(1,1,1),\ (1,1,0),\ (1,0,0),\ (1,0,-1),\ (-1,1,0),\ (-1,1,-1),\ (-1,0,1),\ (-1,0,0)\,.$$

Proof. By (2.1), clearly $a(0,n) = 1$ for all n. The cases of $n = 1$, 2, and 3 yield the triples $(-1,0,0)$, $(1,0,0)$, and $(1,1,0)$, respectively, all of which are listed in the statement of the lemma. Hence assume $n \geq 5$ from now on. Since n is squarefree, there exist $m \in \mathbb{N}$ and prime numbers $p_1 > \ldots > p_m$ such that $n = \prod_{j=1}^m p_j$.

Assume first that $p_m \geq 5$, and for convenience let $\varphi_j = \varphi(p_1 \cdots p_j)$ as well as $a_j = a(1, p_1 \cdots p_j)$, $b_j = a(2, p_1 \cdots p_j)$, and $c_j = a(3, p_1 \cdots p_j)$ for $j \in \{1, \ldots, m\}$. Thus

$$\Phi_{p_1 \cdots p_j}(z) = z^{\varphi_j} + a_j z^{\varphi_j - 1} + b_j z^{\varphi_j - 2} + c_j z^{\varphi_j - 3} + \Psi_j(z)\,,$$

with the appropriate polynomial Ψ_j of degree less than $\varphi_j - 3$. From

$$\Phi_{p_1}(z) = z^{p_1 - 1} + z^{p_1 - 2} + \ldots + z + 1\,,$$

it is clear that $\varphi_1 = p_1 - 1$ and $a_1 = b_1 = c_1 = 1$. On the other hand,

$$\begin{aligned}\Phi_{p_1 \cdots p_j p_{j+1}}(z) &= \frac{\Phi_{p_1 \cdots p_j}(z^{p_{j+1}})}{\Phi_{p_1 \cdots p_j}(z)} \\ &= \frac{z^{p_{j+1}\varphi_j} + a_j z^{p_{j+1}(\varphi_j - 1)} + b_j z^{p_{j+1}(\varphi_j - 2)} + c_j z^{p_{j+1}(\varphi_j - 3)} + \Psi_j(z^{p_{j+1}})}{z^{\varphi_j} + a_j z^{\varphi_j - 1} + b_j z^{\varphi_j - 2} + c_j z^{\varphi_j - 3} + \Psi_j(z)}\,,\end{aligned}$$

which, together with long division and the fact that $p_{j+1} \geq 5$, leads to

$$\begin{aligned}\Phi_{p_1 \cdots p_j p_{j+1}}(z) = z^{(p_{j+1}-1)\varphi_j} - a_j z^{(p_{j+1}-1)\varphi_j - 1} + (a_j^2 - b_j) z^{(p_{j+1}-1)\varphi_j - 2} + \\ + (2a_j b_j - a_j^3 - c_j) z^{(p_{j+1}-1)\varphi_j - 3} + \Psi_{j+1}(z)\,,\end{aligned}$$

and hence in turn yields the recursion $\varphi_{j+1} = (p_{j+1} - 1)\varphi_j$ and

$$a_{j+1} = -a_j\,, \quad b_{j+1} = a_j^2 - b_j\,, \quad c_{j+1} = 2a_j b_j - a_j^3 - c_j\,. \tag{2.3}$$

Using (2.3) with $(a_1, b_1, c_1) = (1,1,1)$ shows that (a_j, b_j, c_j) can have only two different values, namely $(1,1,1)$ if j is odd, and $(-1,0,0)$ if j is even.

Next assume that $p_m = 3$ and hence $m \geq 2$. In this case, (2.3) remains valid for $j \in \{1, \ldots, m-2\}$, yet for $j = m - 1$ it has to be replaced with

$$a_m = -a_{m-1}\,, \quad b_m = a_{m-1}^2 - b_{m-1}\,, \quad c_m = 2a_{m-1}b_{m-1} + a_{m-1} - a_{m-1}^3 - c_{m-1}\,. \tag{2.4}$$

Recall from above that $(a_{m-1}, b_{m-1}, c_{m-1})$ equals either $(1,1,1)$ or $(-1,0,0)$. By (2.4), therefore, the value of (a_m, b_m, c_m) is either $(-1,0,1)$ or $(1,1,0)$.

Finally, if $p_m = 2$ then again $m \geq 2$, and the identity $\Phi_n(z) = \Phi_{p_1 \cdots p_{m-1} 2}(z) = \Phi_{p_1 \cdots p_{m-1}}(-z)$ implies that $a_m = -a_{m-1}$, $b_m = b_{m-1}$, and $c_m = -c_{m-1}$. This yields the remaining four possible values for (a_m, b_m, c_m). □

From (2.1) it is clear that $\Phi_{mn}(z) = \Phi_n(z^m)$, provided that every prime number dividing m also divides n. With this, Lemma 2.1 restricts the possible values for the leading coefficients of Φ_n even in cases where n is not squarefree.

Lemma 2.2. *Assume that $n \in \mathbb{N}$ is not squarefree. Then $a(0,n) = 1$, and the coefficient triple $\big(a(1,n), a(2,n), a(3,n)\big)$ has exactly one of the following five values:*

$$(0,1,0),\ (0,0,1),\ (0,0,0),\ (0,0,-1),\ (0,-1,0)\,.$$

Proof. Pick any prime number p with $p^2 \mid n$. The assertion follows immediately from the fact that $\Phi_n(z) = \Phi_{p\cdot n/p}(z) = \Phi_{n/p}(z^p)$, which, together with Lemma 2.1 and the notation adopted in its proof, implies that $\big(a(1,n), a(2,n), a(3,n)\big)$ equals either $(0, a_m, 0)$, $(0,0,a_m)$, or $(0,0,0)$; recall that $a_m \in \{-1,0,1\}$. □

Remark 2.2. (i) For every squarefree $n \in \mathbb{N}$ the coefficient $a(1,n)$ equals 1 or -1, depending on whether n has an odd or an even number of prime factors; if n is not square free then $a(1,n) = 0$. Thus $a(1,n) = -\mu(n)$, with μ denoting the Möbius function [5, §16.3].

(ii) Put together, Lemmas 2.1 and 2.2 allow for a total of 13 possible patterns for the four leading coefficients of Φ_n. Each pattern occurs for some $n \le 30$, as well as for infinitely many $n \in \mathbb{N}$ thereafter.

Next, note that the actual value of $\Phi_n(\imath)$ can easily be computed.

Lemma 2.3. *Let $n \in \mathbb{N}$. Then $\Phi_n(\imath) \in \mathbb{Z}[\imath]$, and the following holds:*

(i) *If $4 \nmid n$ then $\Phi_n(\imath) \in \{-1, -1+\imath, -\imath, \imath, 1, 1+\imath\}$;*
(ii) *If $4 \mid n$ then*

$$\Phi_n(\imath) = \begin{cases} 0 & \text{if } n = 4\,, \\ p & \text{if } n = 4p^j \text{ for some prime number } p \text{ and } j \in \mathbb{N}\,, \\ 1 & \text{otherwise}\,. \end{cases}$$

Proof. Since Φ_n has integer coefficients, clearly $\Phi_n(\imath) \in \mathbb{Z}[\imath]$ for all n. Also, with $\Phi_1(\imath) = -1+\imath$, $\Phi_2(\imath) = 1+\imath$, and $\Phi_3(\imath) = \imath$, evidently (i) holds for $n \in \{1,2,3\}$. From now on, therefore, let $n \ge 4$. Recall that

$$z^n - 1 = \prod\nolimits_{1\le j\le n : j\mid n} \Phi_j(z) = \Phi_1(z) \prod\nolimits_{2\le j\le n : j\mid n} \Phi_j(z)\,. \tag{2.5}$$

To establish (i), assume first that n is odd. In this case, (2.5) implies that the integer $|\Phi_1(\imath)|^2|\Phi_n(\imath)|^2 = 2|\Phi_n(\imath)|^2$ divides $|\imath^n - 1|^2 = 2$, hence $|\Phi_n(\imath)| = 1$, and $\Phi_n(i) \in \{-1, -\imath, \imath, 1\}$. Next assume that $n \in 2 + 4\mathbb{Z}$. Now (2.5) yields

$$-2 = (-1+\imath)(1+\imath) \prod\nolimits_{3\le j\le n : j\mid n} \Phi_j(\imath)\,,$$

and hence again $|\Phi_n(\imath)| = 1$. This proves (i).

To establish (ii), consider the case of $n \in 4\mathbb{Z}$. Plainly $\Phi_4(\imath) = 0$, so henceforth assume $n \ge 8$. There exist $m \in \mathbb{N}$, prime numbers $p_1 > \ldots > p_m$, and $k_1, \ldots, k_m \in \mathbb{N}$ such that $n = 4\prod_{j=1}^m p_j^{k_j}$. If $p_m \ge 3$ then

$$\Phi_n(\imath) = \Phi_{2p_1\cdots p_m}\left(\imath^{2p_1^{k_1-1}\cdots p_m^{k_m-1}}\right) = \Phi_{2p_1\cdots p_m}(-1) = \Phi_{p_1\cdots p_m}(1)\,.$$

Thus $\Phi_n(\imath) = p_1$ if $m = 1$, and otherwise

$$\Phi_n(\imath) = \Phi_{p_1\cdots p_m}(1) = \frac{\Phi_{p_1\cdots p_{m-1}}(1^{p_m})}{\Phi_{p_1\cdots p_{m-1}}(1)} = 1\,.$$

Similarly, if $p_m = 2$ then

$$\Phi_n(\imath) = \Phi_{p_1\cdots p_m}\left(\imath^{p_1^{k_1-1}\cdots p_{m-1}^{k_{m-1}-1}p_m^{k_m+1}}\right) = \Phi_{p_1\cdots p_m}(1)\,,$$

and again $\Phi_n(\imath) = 2 = p_m$ if $m = 1$, and $\Phi_n(\imath) = 1$ otherwise. □

Remark 2.3. Lemma 2.3(i) allows for a total of six possible values for $\Phi_n(\imath)$. While the two values $-1+\imath$ and $1+\imath$ only occur for $n = 1$ and $n = 2$, respectively, each of the other four values occurs for some $n \le 21$, as well as for infinitely many $n \in \mathbb{N}$ thereafter.

Finally, the polynomial Φ_n, which is irreducible over $\mathbb{Q}$, may remain irreducible when $\mathbb{Q}$ is replaced with a larger field (subfield of the complex numbers $\mathbb{C}$), in particular with a real quadratic number field. Specifically, consider any squarefree integer $d \ge 2$, and let $\widehat{d}$ be the discriminant of the number field $\mathbb{Q}\big(\sqrt{d}\big)$, that is,

$$\widehat{d} = \begin{cases} d & \text{if } d \in 1 + 4\mathbb{Z}\,, \\ 4d & \text{if } d \in \{2,3\} + 4\mathbb{Z}\,. \end{cases}$$

Lemma 2.4. *Let $n \in \mathbb{N}$, and assume that the integer $d \ge 2$ is squarefree. Then the polynomial Φ_n is irreducible over $\mathbb{Q}\big(\sqrt{d}\big)$ if and only if $\widehat{d} \nmid n$.*

Proof. Since the asserted equivalence clearly holds for $n \in \{1,2\}$, let $n \ge 3$ throughout. For every $m \in \mathbb{N}$, denote $\mathbb{Q}(e^{2\pi\imath/m})$ by K_m, for convenience.

Observe first that the irreducibility of Φ_n over $\mathbb{Q}\big(\sqrt{d}\big)$ is equivalent to $\mathbb{Q}\big(\sqrt{d}\big) \cap K_n = \mathbb{Q}$. Indeed, if $\mathbb{Q}\big(\sqrt{d}\big) \subset K_n$ then $\big[\mathbb{Q}\big(\sqrt{d}, e^{2\pi\imath/n}\big) : \mathbb{Q}\big(\sqrt{d}\big)\big] = \frac{1}{2}[K_n : \mathbb{Q}] = \frac{1}{2}\varphi(n) < \varphi(n)$, showing that Φ_n cannot be irreducible over $\mathbb{Q}\big(\sqrt{d}\big)$. If, on the other hand, $\mathbb{Q}\big(\sqrt{d}\big) \not\subset K_n$ then $\mathbb{Q}\big(\sqrt{d}\big) \cap K_n = \mathbb{Q}$ and $\big[K_n\big(\sqrt{d}\big) : K_n\big] = 2$. With this,

$$2\big[\mathbb{Q}\big(\sqrt{d}, e^{2\pi\imath/n}\big) : \mathbb{Q}\big(\sqrt{d}\big)\big] = \big[K_n\big(\sqrt{d}\big) : \mathbb{Q}\big] = \big[K_n(\sqrt{d}) : K_n\big] \cdot [K_n : \mathbb{Q}] = 2\varphi(n)\,,$$

hence $\big[\mathbb{Q}\big(\sqrt{d}, e^{2\pi\imath/n}\big) : \mathbb{Q}\big(\sqrt{d}\big)\big] = \varphi(n)$, which shows that Φ_n is irreducible over $\mathbb{Q}\big(\sqrt{d}\big)$.

It remains to verify that the properties $\mathbb{Q}\big(\sqrt{d}\big) \cap K_n = \mathbb{Q}$ and $\widehat{d} \nmid n$ indeed are equivalent. To this end, recall that $\mathbb{Q}\big(\sqrt{d}\big) \subset K_{\widehat{d}}$. In fact, $m = \widehat{d}$ is the smallest $m \in \mathbb{N}$ such that $\mathbb{Q}\big(\sqrt{d}\big) \subset K_m$; e.g., see [8, Cor.VI.1.2]. Thus, if $\widehat{d} \mid n$ then $\mathbb{Q}\big(\sqrt{d}\big) \subset K_{\widehat{d}} \subset K_n$. Conversely, assume $\widehat{d} \nmid n$ and suppose that $\mathbb{Q}\big(\sqrt{d}\big) \subset K_n$. Then $\mathbb{Q}\big(\sqrt{d}\big) \subset K_{\widehat{d}} \cap K_n = K_m$ with $m = \gcd\big(\widehat{d}, n\big) < \widehat{d}$; e.g., see [14, (11.24)]. This contradiction proves that $\mathbb{Q}\big(\sqrt{d}\big) \cap K_n = \mathbb{Q}$ whenever $\widehat{d} \nmid n$. □

Using the above properties of Φ_n, it is straightforward to identify the minimal polynomials over $\mathbb{Q}$ of trigonometric numbers such as $\cos(\pi r)$ or $\sin(\pi r)$ with $r \in \mathbb{Q}$. Implicitly, this was done already in [11]. However, for the computational proof of Theorem 1.1 put forth in this note, more explicit information is required. Specifically, to identify the minimal polynomial over $\mathbb{Q}$ of $\cos(\pi r)$, say, recall (e.g., from [9, Exc.13.17]) that given any integer $n \ge 0$, there exists a unique monic polynomial $R_n = R_n(z)$ with integer coefficients such that

$$z^n + z^{-n} = R_n(z + z^{-1})\,, \quad \forall z \in \mathbb{C} \setminus \{0\}\,.$$

With this, observe that for every $n \ge 2$ and $z \in \mathbb{C} \setminus \{0\}$,

$$\Phi_{2n}(z) = \sum\nolimits_{j=0}^{\varphi(2n)} a(j,2n) z^{\varphi(2n)-j} = z^{\frac{1}{2}\varphi(2n)} P_n(z + z^{-1})\,, \tag{2.6}$$

with the polynomial $P_n = P_n(z)$ given by

$$P_n(z) = \sum\nolimits_{j=0}^{\frac{1}{2}\varphi(2n)-1} a(j,2n) R_{\frac{1}{2}\varphi(2n)-j}(z) + a\left(\tfrac{1}{2}\varphi(2n), 2n\right) ;$$

in addition, define $P_1(z) = z + 2$. With this, the degree of P_n simply equals p_n, where

$$p_n = \left\{ \begin{array}{ll} 1 & \text{if } n = 1 \\ \frac{1}{2}\varphi(2n) & \text{if } n \geq 2 \end{array} \right\} = \left\{ \begin{array}{ll} 1 & \text{if } n = 1\,, \\ \varphi(n) & \text{if } n \geq 2 \text{ is even}\,, \\ \frac{1}{2}\varphi(n) & \text{if } n \geq 2 \text{ is odd}\,. \end{array} \right. \tag{2.7}$$

For example, $P_2(z) = z$, $P_3(z) = z - 1$, and $P_4(z) = z^2 - 2$. Clearly, each P_n is monic with integer coefficients, and (2.6) implies that P_n is irreducible over a field K with $\mathbb{Q} \subset K \subset \mathbb{C}$ whenever Φ_{2n} is irreducible over K; in particular, P_n is irreducible over $\mathbb{Q}$. Also, by (2.6) and Lemma 2.3,

$$|P_n(0)| = |\Phi_{2n}(i)| = \left\{ \begin{array}{ll} 2 & \text{if } n = 1\,, \\ 0 & \text{if } n = 2\,, \\ p & \text{if } n = 2p^j \text{ for some prime number } p \text{ and } j \in \mathbb{N}\,, \\ 1 & \text{otherwise}\,. \end{array} \right. \tag{2.8}$$

The following, then, is a simple consequence of (2.6) that refines [11, Thm.1].

Proposition 2.1. *Let $r \in \mathbb{Q}$. Then $P_{N(r)}$ is the minimal polynomial over $\mathbb{Q}$ of the number $2(-1)^{1+rN(r)}\cos(\pi r)$. In particular, the degree over $\mathbb{Q}$ of $\cos(\pi r)$ is $p_{N(r)}$.*

Remark 2.4. Fact 1 is an immediate consequence of Proposition 2.1 since, as is easily checked, $p_n = 1$ if and only if $n \in \{1, 2, 3\}$. Note, however, that Fact 1 can also be established in other entirely elementary ways [7]. As a simple corollary, the number $\pi^{-1}\arccos\sqrt{r}$, with $r \in \mathbb{Q}$ and $0 \leq r \leq 1$, is rational if and only if $4r \in \{0, 1, 2, 3, 4\}$; cf. [16].

3. Proof of Theorem 1.1

Fix $r_1, r_2 \in \mathbb{Q}$ such that neither $r_1 - r_2$ nor $r_1 + r_2$ is an integer, and for convenience let $N_j = N(r_j)$ for $j \in \{1, 2\}$, as well as $n_j = p_{N_j}$ and $z_j = 2(-1)^{1+r_j N_j}\cos(\pi r_j)$; plainly, 1, $\cos(\pi r_1)$, and $\cos(\pi r_2)$ are linearly independent over $\mathbb{Q}$ if and only if 1, z_1, and z_2 are.

To see that (i)⇒(ii), simply note that $p_{N(r)} = 1$, and hence $\cos(\pi r) \in \mathbb{Q}$, whenever $N(r) \leq 3$. Thus if 1, z_1, and z_2 are rationally independent then necessarily $N_1, N_2 \geq 4$. Also, from (1.2) it is evident that $(N_1, N_2) \neq (5, 5)$ in this case.

It remains to establish the reverse implication (ii)⇒(i). To this end, assume for the time being that $n_1, n_2 \geq 3$, or equivalently $N_1, N_2 \geq 7$. Then (ii) holds, z_1 and z_2 both are irrational, and the goal is to show that 1, z_1, and z_2 are linearly independent over $\mathbb{Q}$. Assume, therefore, that $rz_1 + sz_2 + t = 0$ with $r, s, t \in \mathbb{Q}$. If $r = 0$ then $s = t = 0$, so assume further that $r \neq 0$, and w.l.o.g. let $r = -1$. Thus, with $s, t \in \mathbb{Q}$ and $s \neq 0$,

$$z_1 = sz_2 + t\,. \tag{3.1}$$

The proof will be complete, at least for the case of $N_1, N_2 \geq 7$, once it is shown that (3.1) always fails. This will now be done by separately considering two cases.

Case I: $t = 0$**.**
Assume first that $t = 0$ in (3.1). Then z_1 and z_2 have the same degree over $\mathbb{Q}$, i.e., $n = n_1 = n_2 \geq 3$, as well as minimal polynomials P_{N_1} and P_{N_2}, respectively. From

$$0 = s^{-n}P_{N_1}(z_1) = s^{-n}P_{N_1}(sz_2) = z_2^n + \ldots + s^{-n}P_{N_1}(0)\,,$$

together with the uniqueness of the (monic) minimal polynomial P_{N_2}, it follows that

$$P_{N_1}(0) = s^n P_{N_2}(0)\,. \tag{3.2}$$

Recall from (2.8) that $|P_{N_j}(0)|$ equals 1 or a prime number. Thus, if $|P_{N_1}(0)| \neq |P_{N_2}(0)|$ then (3.2) is impossible for $s \in \mathbb{Q}$. If, on the other hand, $|P_{N_1}(0)| = |P_{N_2}(0)|$ and (3.2) does have a solution then $|s| = 1$, which in turn implies that

$$\cos(\pi r_1) + \cos(\pi r_2) = 0 \quad \text{or} \quad \cos(\pi r_1) - \cos(\pi r_2) = 0\,.$$

In either case, at least one of the numbers $r_1 - r_2$ and $r_1 + r_2$ is an integer, contradicting the standing assumption that none of them is. In summary, (3.1) fails whenever $t = 0$. In particular, z_1/z_2 is irrational.

Case II: $t \neq 0$**.**
Assume from now on that (3.1) holds with $s, t \in \mathbb{Q}$ and $st \neq 0$. Again, z_1 and z_2 have the same degree over $\mathbb{Q}$, thus $n = n_1 = n_2 \geq 3$. For convenience, let

$$(a_j, b_j, c_j) = \big(a(1, 2N_j), a(2, 2N_j), a(3, 2N_j)\big)\,, \quad j \in \{1, 2\}\,,$$

and consequently

$$P_{N_j}(z) = z^n + a_j z^{n-1} + (b_j - n)z^{n-2} + \big(c_j - a_j(n-1)\big)z^{n-3} + U_j(z)\,, \quad j \in \{1, 2\}\,,$$

where U_j denotes an appropriate polynomial of degree less than $n - 3$. With (3.1), it follows that

$$0 = s^{-n}P_{N_1}(z_1) = s^{-n}P_{N_1}(sz_2 + t) = z_2^n + \widetilde{a}_2 z_2^{n-1} + \widetilde{b}_2 z_2^{n-2} + \widetilde{c}_2 z_2^{n-1} + \widetilde{U}_2(z_2) =: \widetilde{P}_{N_2}(z_2)\,,$$

with a polynomial $\widetilde{U}_2$ of degree less than $n - 3$, and coefficients

$$\widetilde{a}_2 = \frac{nt + a_1}{s}\,,$$

$$\widetilde{b}_2 = \frac{n(n-1)t^2 + 2a_1(n-1)t + 2(b_1 - n)}{2s^2}\,,$$

$$\widetilde{c}_2 = \frac{n(n-1)(n-2)t^3 + 3a_1(n-1)(n-2)t^2 + 6(b_1 - n)(n-2)t + 6c_1 - 6a_1(n-1)}{6s^3}\,.$$

Requiring that $\widetilde{P}_{N_2} = P_{N_2}$ yields

$$\begin{aligned} sa_2 &= nt + a_1\,, \\ 2s^2(b_2 - n) &= n(n-1)t^2 + 2a_1(n-1)t + 2b_1 - 2n\,, \\ 6s^3\big(c_2 - a_2(n-1)\big) &= n(n-1)(n-2)t^3 + 3a_1(n-1)(n-2)t^2 + \\ &\quad + 6(b_1 - n)(n-2)t + 6c_1 - 6a_1(n-1)\,. \end{aligned} \tag{3.3}$$

Note that (3.3) consists of three equations for the two (rational) numbers s and t. Quite plausibly, therefore, (3.3) may be contradictory, which in turn would cause (3.1) to fail also, just as desired. It will now be shown that this indeed is the case, regardless of the actual values of $n \geq 3$ and the coefficient triples (a_j, b_j, c_j). In order to do so, it is convenient to distinguish three subcases, depending on whether none, exactly one, or both of the integers N_j are squarefree.

Case IIa. Assume first that neither N_1 nor N_2 is squarefree. Then, by Lemma 2.2, $a_1 = a_2 = 0$, and the first equation in (3.3) reduces to $0 = nt$, which contradicts the assumption $t \neq 0$. Hence (3.3) fails if neither N_1 nor N_2 is squarefree.

Case IIb. Next, assume that exactly one of the two integers N_1 and N_2 is squarefree; w.l.o.g. let N_2 be squarefree. (Otherwise interchange the roles of z_1 and z_2.) Hence $a_1 = 0$, and by replacing z_2 with $-z_2$ if necessary, it can be assumed that $a_2 = 1$ and consequently, by Lemma 2.1, the pair (b_2, c_2) has exactly one of the following four values:

$$(1, 1),\ (1, 0),\ (0, 0),\ (0, -1)\,. \tag{3.4}$$

In this case, the first equation in (3.3) reads $s = nt$, and the other two equations become

$$\begin{array}{rcl} n(2n^2 + (1-2b_2)n - 1)t^2 - 2(n - b_1) &=& 0\,, \\ n(6n^3 - (5+6c_2)n^2 - 3n + 2)t^3 - 6(n^2 - (2+b_1)n + 2b_1)t + 6c_1 &=& 0\,. \end{array} \tag{3.5}$$

Note that $V_0(n; b_2) = 2n^2 + (1-2b_2)n - 1 \neq 0$ for all $n \geq 3$ and $b_2 \in \{0, 1\}$. It follows that

$$t^2 = \frac{2}{n} \cdot \frac{n - b_1}{V_0(n; b_2)}\,, \tag{3.6}$$

and plugging this into the second equation in (3.5) yields, after a short calculation,

$$t = -\frac{3c_1}{2} \cdot \frac{V_0(n; b_2)}{V_1(n)}\,, \tag{3.7}$$

with the cubic polynomial V_1 given by

$$V_1(z) = (2 + 3b_2 - 3c_2)z^3 + (3 - 2b_1 - 6b_2 - 3b_1b_2 + 3b_1c_2)z^2 - (2 + 3b_1 - 6b_1b_2)z + 2b_1\,.$$

Note that $c_1 \neq 0$ by (3.6) and (3.7), and hence $|c_1| = 1$. Again, it is readily confirmed that $V_1(n) \neq 0$ for all $n \geq 3$ and all relevant values of b_1, b_2, and c_2. In order for (3.6) and (3.7) to be compatible, the (seventh degree polynomial) equation

$$9nV_0(n; b_2)^3 = 8(n - b_1)V_1(n)^2 \tag{3.8}$$

must be satisfied. It is now an elementary task to check that this is not the case for any $n \geq 3$, any $b_1 \in \{-1, 0, 1\}$, and any pair (b_2, c_2) from (3.4). For example, for $b_1 = 1$ and $(b_2, c_2) = (1, 1)$, condition (3.8) takes the form

$$\begin{aligned} 0 &= 40n^7 + 84n^6 - 446n^5 + 347n^4 + 163n^3 - 211n^2 - 9n + 32 \\ &= (n-1)^3(2n+1)^2(10n^2 + 41n - 32)\,, \end{aligned}$$

which for $n \in \mathbb{N}$ only holds if $n = 1$. The altogether eleven other possibilities for b_1 and (b_2, c_2) are dealt with in a completely similar manner. In summary, (3.3) fails if exactly one of the numbers N_1 and N_2 is squarefree.

Case IIc. Finally, assume that both N_1 and N_2 are squarefree. In this case, it can also be assumed that $a_1 = a_2 = 1$, and the pairs (b_1, c_1) and (b_2, c_2) each have exactly one of the four values (3.4). Now the first equation in (3.3) reads $s = nt + 1$, and with this the two other equations reduce to

$$\begin{array}{rcl} (nt+1)^2 &=& \dfrac{V_0(n; b_1)}{V_0(n; b_2)}\,, \\ (nt+1)^3 - 3(nt+1)\dfrac{V_2(n)}{V_4(n)} &=& 2\dfrac{V_3(n)}{V_4(n)}\,, \end{array} \tag{3.9}$$

where the polynomials V_2, V_3, and V_4 are given by

$$\begin{aligned} V_2(z) &= 2z^3 - (3 + 2b_1)z^2 - (3 - 4b_1)z + 2\,, \\ V_3(z) &= (2 + 3b_1 - 3c_1)z^2 + (3 - 6b_1)z - 2\,, \\ V_4(z) &= 6z^3 - (5 + 6c_2)z^2 - 3z + 2\,. \end{aligned}$$

As before, $V_4(n) \neq 0$ for all $n \geq 3$ and $c_2 \in \{-1, 0, 1\}$.

If $b_1 = b_2$ then the first equation in (3.9) yields $nt + 1 \in \{-1, 1\}$, and so $nt = -2$, since $nt = 0$ would contradict the assumption $t \neq 0$. The second equation in (3.9) then becomes

$$0 = V_4(n) + 2V_3(n) - 3V_2(n) = 2(4 + 6b_1 - 3c_1 - 3c_2)n^2 + 12(1 - 2b_1)n - 8\,,$$

which is readily confirmed to not have any integer solution $n \geq 3$ whenever $b_1 = b_2 \in \{0, 1\}$ and $c_1, c_2 \in \{-1, 0, 1\}$.

If, on the other hand, $b_1 \neq b_2$ then in order for the two equations in (3.9) to be compatible, the (tenth degree polynomial) equation

$$V_0(n;b_1)\big(V_0(n;b_1)V_4(n) - 3V_0(n;b_2)V_2(n)\big)^2 = 4V_0(n;b_2)^3V_3(n)^2 \tag{3.10}$$

must be satisfied. Similarly to Case IIb, it is straightforward to check that (3.10) does not hold for any $n \geq 3$ and any two pairs (b_j, c_j) from (3.4) with $b_1 \neq b_2$. For example, if $(b_1, c_1) = (0, -1)$ and $(b_2, c_2) = (1, 1)$ then (3.10) takes the form

$$\begin{aligned} 0 &= 672n^{10} - 48n^9 - 1752n^8 - 20n^7 + 1332n^6 - 92n^5 - 444n^4 + 16n^3 + 48n^2 \\ &= 4n^2(n+1)^2(2n+1)^2(42n^4 - 129n^3 + 141n^2 - 68n + 12)\,, \end{aligned}$$

which has no solution $n \in \mathbb{N}$. The altogether seven other possibilities for (b_1, c_1) and (b_2, c_2) with $b_1 \neq b_2$ are dealt with in a completely similar manner. As a consequence, (3.3) fails whenever N_1 and N_2 are both squarefree. As explained earlier, this completes the proof of the implication (ii)⇒(i) in the case of $N_1, N_2 \geq 7$.

It remains to consider those situations where $N_j \in \{4, 5, 6\}$ for at least one j. Hence assume w.l.o.g. that $N_1 \in \{4, 5, 6\}$, and thus $n_1 = 2$. Clearly, 1, $\cos(\pi r_1)$, and $\cos(\pi r_2)$ are rationally independent unless $n_2 = 2$ as well. Thus both z_1 and z_2 are roots of one of the irreducible polynomials

$$P_4(z) = z^2 - 2\,, \quad P_5(z) = z^2 - z - 1\,, \quad P_6(z) = z^2 - 3\,.$$

If, for instance, $N_1 = 4$ then (3.1) implies that, in analogy to (3.3),

$$0 = s^{-2}P_4(z_1) = s^{-2}P_4(sz_2 + t) = z_2^2 + \frac{2t}{s}z_2 + \frac{t^2 - 2}{s^2} =: \widetilde{P}_4(z_2)\,. \tag{3.11}$$

Note that $\widetilde{P}_4 \neq P_4$ because otherwise (s, t) would equal $(1, 0)$ or $(-1, 0)$, and therefore, as seen earlier, one of the numbers $r_1 - r_2$ and $r_1 + r_2$ would be an integer; but also $\widetilde{P}_4 \neq P_5$ because otherwise $5s^2 = 8$, which is impossible for $s \in \mathbb{Q}$; and $\widetilde{P}_4 \neq P_6$ because otherwise $3s^2 = 2$, which is likewise impossible. The assumption $N_1 = 6$ leads to a similar string of contradictions. In summary, this shows that (3.1) cannot hold whenever $N_1, N_2 \in \{4, 5, 6\}$ but $(N_1, N_2) \neq (5, 5)$, and hence completes the proof of Theorem 1.1. □

Remark 3.5. The special role played by the case of $N_1 = N_2 = 5$ in the above argument is highlighted by the fact that, in analogy to (3.11),

$$s^{-2}P_5(sz + t) = z^2 + \frac{2t - 1}{s}z + \frac{t^2 - t - 1}{s^2} =: \widetilde{P}_5(z)\,,$$

and $\widetilde{P}_5 = P_5$ for $(s, t) = (-1, 1)$. This also explains the validity of (1.2).

The argument given above does not depend on the underlying field being $\mathbb{Q}$. The same reasoning applies over larger fields, provided that P_n remains irreducible, and (3.2) has no solution with $|s| \neq 1$. Theorem 1.1 can thus be strengthened without further effort.

Theorem 3.2. *Let $r_1, r_2 \in \mathbb{Q}$ be such that neither $r_1 - r_2$ nor $r_1 + r_2$ is an integer, and assume that the integer $d \geq 2$ is squarefree with $\gcd\big(d, N(r_j)\big) = 1$ for $j \in \{1, 2\}$. Then the following are equivalent:*

(i) *The numbers 1, $\cos(\pi r_1)$, and $\cos(\pi r_2)$ are linearly independent over $\mathbb{Q}\big(\sqrt{d}\big)$;*
(ii) *$N(r_j) \geq 4$ for $j \in \{1, 2\}$, and $\big(N(r_1), N(r_2)\big) \neq (5, 5)$.*

Proof. Since linear independence over $\mathbb{Q}\big(\sqrt{d}\big)$ implies rational independence, the implication (i)⇒(ii) is obvious from Theorem 1.1. To see the converse, observe that if d and $N(r)$ are coprime then $\widehat{d} \nmid 2N(r)$, and hence $P_{N(r)}$, the minimal polynomial over $\mathbb{Q}$ of

$2(-1)^{1+rN(r)}\cos(\pi r)$, is irreducible over $\mathbb{Q}\big(\sqrt{d}\big)$, as a consequence of (2.6) and Lemma 2.4. In particular, $\cos(\pi r)$ has the same degree $p_{N(r)}$ over $\mathbb{Q}\big(\sqrt{d}\big)$ as it has over $\mathbb{Q}$. Furthermore, notice that if $|P_{N(r_1)}(0)| \neq |P_{N(r_2)}(0)|$ then (3.2) has no solution s in $\mathbb{Q}\big(\sqrt{d}\big)$ since the degree over $\mathbb{Q}$ of s is at least 3. Thus when $\mathbb{Q}$ is replaced with $\mathbb{Q}\big(\sqrt{d}\big)$, the proof of (ii)⇒(i) carries over verbatim from the proof of Theorem 1.1. □

To put Theorem 3.2 into perspective, note that with $r_1 = \frac{1}{8}$ and $r_2 = \frac{3}{8}$, the numbers $\cos(\pi r_1)$ and $\cos(\pi r_2)$, though rationally independent by Theorem 1.1, are linearly dependent over $\mathbb{Q}\big(\sqrt{2}\big)$, since $\cos(3\pi/8) = (\sqrt{2}-1)\cos(\pi/8)$. This is consistent with the fact that $N(r_1) = N(r_2) = 8$ is divisible by $d = 2$. Thus the implication (ii)⇒(i) in Theorem 3.2 may fail if d and $N(r_j)$ have a common factor. Conversely, the numbers 1, $\cos(\pi r_1)$, and $\cos(\pi r_2)$ may well be independent over $\mathbb{Q}\big(\sqrt{d}\big)$ even in cases where $\gcd\big(d, N(r_j)\big) \neq 1$. To see this, take for instance $r_1 = \frac{1}{16}$ and $r_2 = \frac{7}{16}$. Again $d = 2$ divides $N(r_1) = N(r_2) = 16$, and yet the numbers 1, $z_1 = 2\cos(\pi/16)$, and $z_2 = 2\cos(7\pi/16)$ are linearly independent over every real quadratic field. This follows easily from the fact that the minimal polynomial over $\mathbb{Q}\big(\sqrt{d}\big)$ of both z_1 and z_2 equals P_{16} if $d \neq 2$, and equals $z^4 - 4z^2 + 2 - \sqrt{2}$ if $d = 2$.

Acknowledgements. The author was supported by an NSERC Discovery Grant. He is much indebted to S. Gille and A. Weiss for helpful discussions and comments. He also wishes to thank J. Calcut and G. Molteni for bringing several important references to his attention, and an anonymous referee for suggestions that helped improve the exposition of this note.

REFERENCES

[1] Bachman, G., *On the coefficients of cyclotomic polynomials*, Mem. Amer. Math. Soc., No. 510, (1993)
[2] Calcut, J. S., *Rationality and the Tangent Function*, preprint available at `http://www.oberlin.edu/faculty/jcalcut/papers.htm`, accessed 26 April 2017
[3] Conway, J. H. and Jones, A. J., *Trigonometric Diophantine equations (On vanishing sums of roots of unity)*, Acta Arith., **30** (1976), 229–240
[4] Fröhlich, A. and Taylor, M. J., *Algebraic number theory*, Cambridge University Press, 1991
[5] Hardy, G. H. and Wright, E. M., *An Introduction to the Theory of Numbers*, fourth ed., Clarendon Press, Oxford, 1960
[6] Hungerford, T. W., *Algebra*, Graduate Texts in Mathematics, No. 73, Springer, 1974
[7] Jahnel, J., *When is the (co)sine of a rational angle equal to a rational number?*, preprint `arXiv 1006.2938`, 2010
[8] Janusz, G. J., *Algebraic Number Fields*, Academic Press, 1973
[9] Kunz, E., *Algebra*, Vieweg, 1991
[10] Lam, T. Y. and Leung, K. H., *On vanishing sums of roots of unity*, J. Algebra, **224** (2000), 91–109
[11] Lehmer, D. H., *A note on trigonometric algebraic numbers*, Amer. Math. Monthly, **40** (1933), 165–166
[12] Mann, H. B., *On linear relations between roots of unity*, Mathematika, **12** (1965), 107–117
[13] Niven, I., *Irrational numbers*, Carus Monographs, No. 11, The Mathematical Association of America, 1956
[14] Stroth, G., *Algebra*, de Gruyter, 1998
[15] Underwood, R. S., *On the irrationality of certain trigonometric functions*, Amer. Math. Monthly, **28** (1921), 374–376
[16] Varona, J. L., *Rational values of the arccosine function*, Cent. Eur. J. Math., **4** (2006), 319–322

UNIVERSITY OF ALBERTA
MATHEMATICAL AND STATISTICAL SCIENCES
EDMONTON, ALBERTA, CANADA
E-mail address: `berger@ualberta.ca`