Hang Lung Mathematics Awards
Vol. 4 (2010)

Hang Lung Mathematics Awards 2010

Gold Award

Expressibility of Cosines as Sum of Basis

Team Members: Kwok Wing Tsoi, Ching Wong
Teacher: Mr. Yan Ching Chan
School: Po Leung Kuk Centenary Li Shiu Chung Memorial College

Hang Lung Mathematics Awards
Vol. 4 (2010), pp. 1–24

EXPRESSIBILITY OF COSINES AS SUM OF BASIS

TEAM MEMBERS
Kwok Wing Tsoi, Ching Wong

TEACHER
Mr. Yan Ching Chan

SCHOOL
Po Leung Kuk Centenary Li Shiu Chung Memorial College

Abstract. The central issue we are investigating is based on a problem from The Hong Kong (China) Mathematical Olympiad. It is basically about whether a cosine ratio is expressible as a sum of rational numbers to powers of reciprocals of primes. In our project, we give the generalization of this problem by using some tricks in elementary Number Theory and Galois Theory.

1. The Contest Problem

The central issue we are investigating is based on a problem from The Hong Kong (China) Mathematical Olympiad. The problem is about whether a trigonometric ratio is expressible in a certain form. Studying forms of numbers is indeed an active research aspect in Number Theory. Being maniacs in Number Theory, we have been deeply inspired by the elementary solution given by our trainer. Therefore, we attempted to generalize the problem.

In this chapter, we would state the original problem as well as the generalization we wish to attain. We also showed how we tackled the small prime cases by elementary technique and the difficulties of large prime cases through such means.

1.1. The original problem, the case $p = 7$

Here comes the original problem, proposed by Dr. Li Kin Yin from HKUST.

THIS PROJECT IS GENEROUSLY SUPERVISED AND ADVISED BY **DR.KOOPA KOO TAK LUN** FROM INTERNATIONAL MATHEMATICAL OLYMPIAD HONG KONG COMMITTEE. THE CONTEST PROBLEM IS DUE TO **DR.LI KIN YIN** FROM HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY.

Problem 1. *(CHKMO). Prove that* $\cos\dfrac{2\pi}{7}$ *is not of the form* $p+\sqrt{q}+\sqrt[3]{r}$*, where* p, q *and* r *are rational numbers.*

Proof. (Due to Dr. Li)
Let $\omega = \cos\dfrac{2\pi}{7} = 2\cos^2\dfrac{\pi}{7} - 1$. As $\cos\dfrac{2\pi}{7} > 0$, we have $\cos\dfrac{\pi}{7} = \sqrt{\dfrac{1+\omega}{2}}$.

Using the fact that $\cos\dfrac{4\pi}{7} + \cos\dfrac{3\pi}{7} = 0$, then transforming it by trigonometric identity,

$$\implies 2\cos^2\frac{\pi}{7} - 1 + 4\left(\cos\frac{\pi}{7}\right)^3 - 3\cos\frac{\pi}{7} = 0,$$

by substituting the above terms,

$$\begin{aligned}
\implies \quad & 2\omega^2 - 1 + 4\left(\frac{1+\omega}{2}\right)^{\frac{3}{2}} - 3\left(\frac{1+\omega}{2}\right)^{\frac{1}{2}} = 0 \\
\implies \quad & \sqrt{\frac{1+\omega}{2}}(2(1+\omega) - 3) = 1 - 2\omega^2,
\end{aligned}$$

simplifying we have,

$$\begin{aligned}
\implies \quad & (1+\omega)(4\omega^2 - 4\omega + 1) = 2 - 8\omega^2 + 8\omega^4 \\
\implies \quad & 8\omega^4 - 4\omega^3 - 8\omega^2 + 3\omega + 1 = 0
\end{aligned}$$

As $\omega = 1$ is a trivial root, after factorization, we have

$$(\omega - 1)(8\omega^3 + 4\omega^2 - 4\omega - 1) = 0$$

Then we let $P(x) = 8x^3 + 4x^2 - 4x - 1$, by **Rational Root Theorem**,

$$\begin{aligned}
P(1) &= 8 + 4 - 4 - 1 = 7 \neq 0 \\
P(-1) &= -8 + 4 + 4 - 1 = -1 \neq 0 \\
P(\frac{1}{2}) &= 1 + 1 - 2 - 1 = -1 \neq 0 \\
P(-\frac{1}{2}) &= -1 + 1 + 2 - 1 = 1 \neq 0 \\
P(\frac{1}{4}) &= \frac{1}{8} + \frac{1}{4} - 1 - 1 = -\frac{13}{8} \neq 0 \\
P(-\frac{1}{4}) &= -\frac{1}{8} + \frac{1}{4} + 1 - 1 = \frac{1}{8} \neq 0 \\
P(\frac{1}{8}) &= \frac{1}{64} + \frac{1}{16} - \frac{1}{2} - 1 = -\frac{91}{64} \neq 0 \\
P(\frac{1}{8}) &= -\frac{1}{64} + \frac{1}{16} + \frac{1}{2} - 1 = -\frac{29}{64} \neq 0
\end{aligned}$$

Therefore, $P(x) = 0$ has no rational roots.

Assume ω is of the form $p+\sqrt{q}+\sqrt[3]{r}$, then ω is a root of $Q(x) = (x-p-\sqrt{q})^3 - r$. The coefficients of $Q(x)$ are in $K = \{a+b\sqrt{q} | a, b \in \mathbb{Q}\}$. Since $q \geq 0$, the coefficient of x in $Q(x)$ is $3(p^2+q+2p\sqrt{q})$, which is non-negative and irrational. However, the coefficient of x in $P(x)$ is -4. Hence $P(x) \neq 8Q(x)$.

Let $R(x) = P(x) - 8Q(x)$. Since $R(\omega) = P(\omega) - 8Q(\omega) = 0$, ω is a root of $R(x) = 0$, whose degree is 1 or 2, and the coefficients of it are in K.

Case 1. If $deg(R(x)) = 1$, we let $R(x) = mx + n$. As m, n are in K, $\omega = -\dfrac{n}{m}$ is also in K. (Here, we used a trivial fact that K is closed under division.)

Case 2. If $deg(R(x)) = 2$ and $R(x)$ is a factor of $P(x)$ in $K[x]$, consider $G(x) = \dfrac{P(x)}{R(x)}$, then we have $deg((G(x)) = 1$ and $G(x) \in K[x]$. Therefore, the root of $G(x) = 0$ is in K, which is also a root of $P(x) = 0$.

Case 3. If $deg(R(x)) = 2$ and $R(x)$ is not a factor of $P(x)$ in $K[x]$, let $r(x)$ be the remainder when $P(x)$ is divided by $R(x)$. Since $P(\omega) = R(\omega) = 0$, clearly $r(\omega) = 0$. According to Division Algorithm, $deg(r(x)) = 1$ and the coefficients of ot are in K. Therefore, ω is again in K.

In all three cases, $P(x)$ has a root in K. Since $P(x)$ does not have rational roots, $P(x)$ has an irrational root in K. Then $P(x)$ is a product of degree 1 polynomial and a degree 2 polynomial with both having rational coefficients. The degree 1 factor yields a rational root for $P(x)$, which is absurd. Therefore, ω cannot of the form $p+\sqrt{q}+\sqrt[3]{r}$. □

The central idea of this proof is making use of the **Rational Root Theorem**. Therefore, we state its statement and the proof here [See reviewer's comment (3)].

Theorem 2. *(Rational Root Theorem). If*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

and $f\left(\dfrac{p}{q}\right) = 0$*, where* $p, q \in \mathbb{Z}$ *and* $(p, q) = 1$*, then* p *divides* a_0 *and* q *divides* a_n*.*

Proof. As $f\left(\dfrac{p}{q}\right) = 0$, multiplying both side by q^{n-1}, we have

$$q^{n-1} f\left(\frac{p}{q}\right) = \frac{a_n p^n}{q} + N = 0,$$

where $N \in \mathbb{Z}$. Therefore, $\dfrac{a_n p^n}{q} \in \mathbb{Z}$. As $(p, q) = 1$, we have $q \mid a_n$, as desired.

Then, we consider

$$\begin{aligned} q^n f\left(\frac{p}{q}\right) =& a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0 \\ \implies \qquad a_0 q^n =& -p(a_n p^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1 q^{n-1}). \end{aligned}$$

Therefore, $p \mid a_0 q^n$. As $(p, q) = 1$, we have $p \mid a_0$. We are done. □

After working on this CHKMO problem, we then doubted whether, in general, $\cos\dfrac{2\pi}{p}$, where p is a prime, is expressible as sum of rational numbers to the power of reciprocal of primes. We first give the statement of our thought mathematically.

Theorem 3. *Let p be an odd prime, then $\cos\dfrac{2\pi}{p} = a_0 + a_1 + a_2 + \cdots + a_k$ for some $k \in \mathbb{Z}$, where $a_i = d_i^{1/p_i}$, $p_i = i$th prime, $a_0, d_i \in \mathbb{Q}$, if and only if $p = 3$ or 5.*

The final goal of our project is to prove this theorem.

1.2. The case $p = 3$ and $p = 5$

Here we prove the sufficiency of our conjecture, which is relatively easy.

The case $p = 3$ is trivial as $\cos\dfrac{2\pi}{3} = -\dfrac{1}{2}$.

When $p = 5$, let $\omega = \cos\dfrac{2\pi}{5}$. Substituting $\theta = \dfrac{2\pi}{5}$ into

$$\cos 5\theta = 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta,$$

we have

$$1 = 16\omega^5 - 20\omega^3 + 5\omega.$$

As $\omega = 1$ is a trivial root, factorized we have,

$$\begin{aligned} \implies & (\omega - 1)(16\omega^4 + 16\omega^3 - 4\omega^2 - 4\omega + 1) = 0 \\ \implies & 16\omega^2 + 16\omega - 4 - \frac{4}{\omega} + \frac{1}{\omega^2} = 0 \\ \implies & \left(4\omega - \frac{1}{\omega}\right)^2 + 4\left(4\omega - \frac{1}{\omega}\right) + 4 = 0 \\ \implies & \left(4\omega - \frac{1}{\omega} + 2\right)^2 = 0 \\ \implies & 4\omega^2 + 2\omega - 1 = 0, \text{ as } \omega \neq 0 \\ \implies & \omega = \frac{-1 \pm \sqrt{5}}{4} \end{aligned}$$

As $0 < \omega < 1$, $\omega = \dfrac{-1+\sqrt{5}}{4} = -\dfrac{1}{4} + \sqrt{\dfrac{5}{16}}$, as desired.

1.2.1. Failure, the case $p = 11$

We have tackled the cases $p = 3, 5$ and 7. The next one we want to deal with is $p = 11$. Without any constructive thoughts, we thus tried to work similarly to the original solution as follows,

When $p = 11$, we let $\omega = \cos\dfrac{2\pi}{11}$, then $\cos\dfrac{\pi}{11} = \sqrt{\dfrac{1+\omega}{2}}$.
Using the facts that $\cos 5\theta = 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta$ and $\cos\dfrac{5\pi}{11} + \cos\dfrac{6\pi}{11} = 0$, we have

$$\begin{aligned} & 16\left(\frac{\omega+1}{2}\right)^{\frac{5}{2}} - 20\left(\frac{\omega+1}{2}\right)^{\frac{3}{2}} + 5\left(\frac{\omega+1}{2}\right) + 4\omega^3 - 3\omega = 0 \\ \implies & \left(\frac{\omega+1}{2}\right)^{\frac{1}{2}}(4\omega^2 - 2\omega - 1) = 3\omega - 4\omega^3 \\ \implies & (\omega-1)(32\omega^5 + 16\omega^4 - 32\omega^3 - 12\omega^2 + 6\omega + 1) = 0 \end{aligned}$$

We then similarly let $P(x) = 32x^5 + 16x^4 - 32x^3 - 12x^2 + 6x + 1$.

Assume ω is of the form $p + \sqrt{q} + \sqrt[3]{r} + \sqrt[5]{s}$, then ω is a root of

$$Q(x) = (x - p - \sqrt{q} - \sqrt[3]{r})^5 - s.$$

The coefficients of $Q(x)$ are in

$$K = \{a_0 + a_1\sqrt{q} + 1 + 2\sqrt[3]{r} + a_3\sqrt[3]{r^2} + a_4\sqrt{q}\sqrt[3]{r} + a_5\sqrt{q}\sqrt[3]{r^2} : a_i \in \mathbb{Q}\}.$$

Unfortunately, this seems to be abysmally complicated.

Therefore, we understand that it is almost impossible to attain the generalization by elementary means. It is a must to seek alternative, or even advanced methods. Knowing that we are struggling at this critical point, one of our trainers at IMOHK, Dr. Koopa Koo Tak-Lun suggested us to study the Field Theory and Galois Theory. He sensed that theories on those aspects may be a possible path for us to reach the ultimate goal.

Indeed, we finally proved our conjecture using Galois Theory, without any painful or tedious calculation.

2. Essential background

In this chapter, we would go over all the necessary knowledge and theories we need in attaining the generalization. This includes the Field Theory and Galois Theory. Proofs of some theorems have been omitted to avoid redundancy.

2.1. Field Theory

In elementary terms, a **field** is defined as a commutative ring with identity such that non-zero elements form a group under multiplication.

Example 4. $\mathbb{Q}, \mathbb{R}$ *and* $\mathbb{C}$ *are familiar examples of fields. In our project, fields like* $\mathbb{Q}(\zeta_p)$ *and* $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ *also appear frequently. (In this project, the notation* ζ_n *denotes the primitive n-th roots of unity.)*

Definition 5. *(Field extension). If* $F \subseteq K$ *are fields, then* K *is called a field extension of* F*. We denote the degree of* K/F *by* $[K : F]$*. If* $[K : F] < \infty$*, then* K *is called a finite extension of* F*. In particular, finite field extensions of* $\mathbb{Q}$ *are called* algebraic number fields*.*

The degree of K/F indeed means the dimension of K as an F-vector space. Also, it denotes the degree of the minimal polynomial, which is defined as following.

Definition 6. *(Minimal Polynomial). The minimal polynomial of an element* α *over* F *is defined as the monic polynomial* $f \in F[x]$ *such that* f *is irreducible over* F *and* $f(\alpha) = 0$*.*

Example 7. *Since the minimal polynomial of* $\sqrt{2}$ *over* Q *is* $x^2 - 2 = 0$*, it implies* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$*.*

Degree consideration plays an important role in our proof. The central theorem involved is called the *Tower Law*, which gives the relationship of degree in a series of field extensions. It is a very convenient way for us to evaluate the degrees of some sub-extensions along a field diagram.

Theorem 8. *(Tower Law). Given* M/L *and* L/K *be field extensions, then*

$$[M : K] = [M : L][L : K]$$

Proof. If either M/L or L/K is an infinite extension, then M contains infinitely many independent vectors over K. Hence M/K is also an infinite extension, and so both sides of the equation are infinite and therefore equal.

$$\begin{array}{c} M \\ \Big| \text{ basis } \{r_i\} \\ L \\ \Big| \text{ basis } \{s_i\} \\ K \end{array}$$

Otherwise M/L and L/K are both finite extensions. Let $r_1, r_2, \ldots, r_p$ be a basis for M/L and let $s_1, s_2, \ldots, s_q$ be a basis for L/K. Then

$$RHS = [M : L][L : K] = pq.$$

We are going to show that $r_i s_j$ forms a basis for M/K, since then

$$[M : K] = pq = RHS.$$

First, we check that $r_i s_j$ spans. Pick $m \in M$, since $r_1, r_2, \ldots, r_p$ is a basis for M/L, we may find $a_1, a_2, \ldots a_p \in L$ such that

$$m = a_1 r_1 + a_2 r_2 + \cdots + a_p r_p.$$

On the other hand, as $s_1, s_2, \ldots, s_q$ is a basis for L/K, $\forall a_i \in L$, we may find $b_{i1}, b_{i2}, \ldots, b_{iq} \in K$ such that

$$a_i = b_{i1} s_1 + b_{i2} s_2 + \cdots + b_{iq} s_q$$

Then, we have

$$\begin{aligned} m =& (b_{11} s_1 + b_{12} s_2 + \cdots + b_{1q} s_q) r_1 + \cdots + (b_{p1} s_1 + b_{p2} s_2 + \cdots + b_{pq} s_q) r_p \\ =& b_{11}(s_1 r_1) + b_{12}(s_2 r_1) + \cdots + b_{pq}(s_q r_p). \end{aligned}$$

Therefore, m is a linear combination of $r_i s_j$ over K, i.e. $r_i s_j$ spans M/K.

Second, we shall check that $r_i s_j$ is linearly independent over K. Suppose

$$b_{11}(s_1 r_1) + b_{12}(s_2 r_1) + \cdots + b_{pq}(s_q r_p) = 0$$

for some $b_{ij} \in K$. Then

$$(b_{11} s_1 + b_{12} s_2 + \cdots + b_{1q} s_q) r_1 + \cdots + (b_{p1} s_1 + b_{p2} s_2 + \cdots + b_{pq} s_q) r_p = 0$$

Since $r_1, r_2, \ldots, r_p$ are linearly independent over L, we have

$$b_{i1} s_1 + b_{i2} s_2 + \cdots + b_{iq} s_q = 0$$

for all $i = 1, 2, \ldots, p$. By linear independence of $s_1, s_2, \ldots, s_q$ over K again, $b_{ij} = 0$ for all i and j.

Thus, $r_i s_j$ is a basis for M/K. □

As mentioned, one of the critical thoughts for us to attain the generalization is to investigate the field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and its extension $\mathbb{Q}(\zeta_p)$, where p is a prime. The following is to derive the degrees of these fields over $\mathbb{Q}$, using some classical tricks in elementary number theory.

Theorem 9. *(Eisenstein's Irreducibility Criterion). Let*

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

be a polynomial over a commutative unique factorization domain R. If there exists a prime $p \in R$ such that (i) $p \mid a_{n-1}, \ldots, a_0$, (ii) $p \nmid a_n$ and (iii) $p^2 \nmid a_0$, then $f(x)$ is irreducible over R.

Proof. Suppose $f(x) = (b_0+b_1x+\cdots+b_px^p)(c_0+c_1x+\cdots+c_qx^q)$, where $p, q \in (0, n)$. Since $a_0 = b_0c_0$, we have $p \mid b_0c_0$ and $p^2 \nmid b_0c_0$. Hence, p divides one but not both of b_0 and c_0. WLOG, assume $p \mid b_0$ and $p \nmid c_0$. Since $p \mid a_{n-1}m \ldots, a_0$ and $p \nmid a_n$, there exist b_i such that $p \nmid b_i$. Let k be the smallest index such that $p \nmid b_k$. Let $m = \max\{k, q\}$. Consider $a_k = b_kc_0 + b_{k-1}c_1 + \cdots + b_{k-m}c_m$ is divisible by p. Note that p divides $(b_{k-1}c_1 + \cdots + b_{k-m}c_m)$ but does not divide b_kc_0, which yields a contradiction. □

Lemma 10. *If p is a prime, then p divides $\binom{p}{r}$, where $0 < r < p$.*

Proof. Let $N = \binom{p}{r} = \frac{p}{r}\binom{p-1}{r-1}$. Therefore, $rN = p\binom{p-1}{r-1} \equiv 0 \pmod{p}$. As p is a prime and $0 < r < p, (p, r) = 1$. The cancellation law asserts that $N \equiv 0 \pmod{p}$. We are done. □

Theorem 11. *If p is a prime, then $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.*

Proof. Consider the polynomial $f(x) = x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x + 1)$. We claim that $g(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$, and hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = deg(g(x)) = p - 1$. We know that $g(x)$ is irreducible iff $g(x + 1)$ is irreducible. However,

$$\begin{aligned} g(x+1) =& (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1) + 1 \\ =& \sum_{i=0}^{p-1} \left(\binom{p-1}{i} + \binom{p-2}{i} + \cdots + \binom{i}{i} \right) x^i \\ =& \sum_{i=0}^{p-1} \binom{p}{i+1} x^i \end{aligned}$$

Using **Lemma 10**, all coefficients of $g(x + 1)$ except the leading coefficient are divisible by p, and the constant term is p, which is not divisible by p^2. Eisenstein's Irreducibility Criterion asserts that $g(x + 1)$ is irreducible over $\mathbb{Q}$. Hence, $g(x)$ is irreducible over $\mathbb{Q}$. □

Theorem 12. *If p is a prime, then* $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \dfrac{p-1}{2}$.

Proof. Clearly, $\mathbb{Q}(\zeta_p)$ is a field extension of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. Consider the following field diagram.

$$\begin{array}{c} \mathbb{Q}(\zeta_p) \\ | \\ \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \\ | \\ \mathbb{Q} \end{array}$$

We know that ζ_p is complex while $\zeta_p + \zeta_p^{-1}$ is real, which implies $\mathbb{Q}(\zeta_p) \neq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})] = 2$. With $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, the Tower Law asserts that $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \dfrac{p-1}{2}$. □

2.2. Galois Theory

Another essential tool in our project is Galois Theory. To define what Galois extensions are, two important concepts should be introduced, the splitting field and separable polynomial.

Definition 13. *The extension L/F is called a splitting field for $f(x) \in F[x]$ if L is the smallest field that contains all roots of $f(x) \in F(x)$.*

Example 14. *$\mathbb{Q}(\sqrt{2})$ is the splitting field of $f(x) = x^2 - 2$, because it is clearly the smallest field containing the two roots of f, namely $\pm\sqrt{2}$.*

Definition 15. *A polynomial over F is called* **separable** *if all its roots are distinct. Otherwise, it is* **inseparable**.

With these definitions, we can now state what Galois extensions are.

Definition 16. *A finite field extension E/F is* **Galois** *if E is a splitting field of some separable polynomial $f(x) \in F[x]$.*

Example 17. *$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is clearly Galois because $\mathbb{Q}(\sqrt{2})$ splits over $\mathbb{Q}$. However, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois because $\zeta_3 \notin \mathbb{Q}(\sqrt[3]{2})$, i.e. $\mathbb{Q}(\sqrt[3]{2})$ does not split over $\mathbb{Q}$.*

Definition 18. *(Galois Group). Let K be a field extension of F. The Galois group $Gal(K/F)$ is the set of all F-automorphisms of K.*

Example 19. *$Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ contains two functions, namely id and σ, where id denotes the identity map and σ denotes the conjugation map, i.e. sending $\sqrt{2}$ to $-\sqrt{2}$. Moreover, for all natural numbers n, $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma_i : (i,n) = 1\}$, where σ_i is defined by $\sigma_i(\alpha) = \alpha^i$. [See reviewer's comment (4)]*

Theorem 20. *For all natural numbers n,*

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times \text{ and } [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n).$$

[See reviewer's comment (5)]

We shall omit the proof of this renowned isomorphism and interpret some useful results based on it.

Lemma 21. *Let p be a prime, then $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.*

Proof. Suppose not, let $l =$ be the l.c.m. of the order of a as a runs through $(\mathbb{Z}/p\mathbb{Z})^\times$. Then by assumption, we have $l < p-1$. (otherwise, there exists an element with order $p-1$.) However, we also have $a^l \equiv 1 \pmod{p}$ for all a. Therefore, the equation $x^l - 1 \equiv 0 \pmod{p}$ has more than l solutions. This is a contradiction. □

Theorem 22. *If p is an odd prime, then $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a cyclic group.*

Proof. Using **Theorem 20**, $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Moreover, since p is an odd prime, according to the previous lemma, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic. We are done. □

[See reviewer's comment (6)]

Theorem 23. *A finite normal extension K is cyclic over F if $Gal(K/F)$ is a cyclic group.*

1. *If K is cyclic over F and E is a normal extension of F, where $F \leq E \leq K$, then E is cyclic over F and K is cyclic over E.*
2. *If K is cyclic over F, then there exists unique field E, $F \leq E \leq K$, of degree d over F for each divisor d of $[K : F]$.*

Proof. (Due to John B. Fraleigh)
(For 1.) Since K/F is a cyclic extension, by definition, $Gal(K/F)$ is a cyclic group. As $Gal(K/E) \leq Gal(K/F)$, it implies $Gal(K/E)$ is also cyclic $\implies$ K/E is also cyclic extension. Since E is a normal extension of F, the Third Isomorphism Theorem asserts that $Gal(E/F) \cong Gal(K/F)/Gal(K/E)$ so $Gal(E/F)$ is isomorphic to a factor group of cyclic group, and is thus cyclic. Therefore, E is cyclic over F.

(For 2.) By Galois Theory, we know that there is a one-to-one correspondence between subgroups H of $Gal(K/F)$ and fields $E = K_H$ such that $F \leq E \leq K$. Because $Gal(K/F)$ is cyclic, it contains precisely one subgroup of each order d that

divides $[Gal(K/F)] = [K : F]$. Such a subgroup corresponds to a field E where $F \leq E \leq K$ and $[K : E] = d$, so that $[E : F] = m = n/d$. Now as d runs through all divisors of n, the quotients $m = n/d$ also run through all divisors of n, so we are done. □

The following theorem illustrates the relationship of a Galois extension and its sub-extensions.

Theorem 24. *If K/F is a Galois and abelian extension, then all the sub-extensions between them are Galois.*

Since $(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ is abelian, **Theorem 24** asserts that all the sub-extensions of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ are Galois.

Another key to attain the generalization is the application of norm. We first give the definition of norm.

Definition 25. *If K/F is Galois with Galois group G, then for all $a \in K$, the* **norm** *is given by $N_{K/F}(a) = \prod_{\sigma \in G} \sigma(a)$.*

Example 26. *Consider $\mathbb{Q}(i)/\mathbb{Q}$, the norm of $z = a + bi \in \mathbb{Q}(i)$ is given by*

$$N(a + bi) = (a + bi)\sigma(a + bi) = (a + bi)(a - bi) = a^2 + b^2$$

Theorem 27. *(Properties of norm) The norm is multiplicative, i.e.*

$$\text{for all } \alpha, \beta \in E,\ N_{E/F}(\alpha)N_{E/F}(\beta) = N_{E/F}(\alpha\beta).$$

Moreover, for all $a \in F$, $N_{E/F}(a) = a^{[E:F]}$.

Proof. For the later part, since $a \in F$, we have $\sigma_n(a) = a$, for all $\sigma_n \in Gal(E/F)$. Thus, $N_{K/F}(a) = \prod_{\sigma \in G} \sigma(a) = a^{[Gal(E/F)]} = a^{[E:F]}$. We are done. □

Theorem 28. *If $\sigma_i \in Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, then $\sigma_i(N_{E/F}(\alpha)) = N_{E/F}(\alpha)$ for all $\alpha \in E$.*

Proof. Let $G = Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Recall the definition of **norm**, $N_{K/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$. Therefore, for all $\sigma_i \in G$, $\sigma_i(N_{K/F}(\alpha)) = \sigma_i(\prod_{\sigma \in G} \sigma(\alpha))$. Since G is a group, the factors on the right-hand side are permutated under composition of sigma-functions. i.e. if $G = \{\sigma_1, \ldots, \sigma_n\}$, then

$$\sigma_i(G) = \{\sigma_i\sigma_1, \ldots, \sigma_i\sigma_n\} = \{\sigma_1, \ldots, \sigma_n\} = G.$$

Thus, $\sigma_i(N_{K/F}(\alpha)) = \sigma_i(\prod_{\sigma \in G} \sigma(\alpha)) = \sigma(\alpha)$. We are done. □

The above is a rough collection of concepts and theorems which we will use in order to prove our conjecture. In the following chapter, we would attempt to re-solve the contest problem by Galois Theory, followed by the proof of our generalization.

3. Success to the generalization

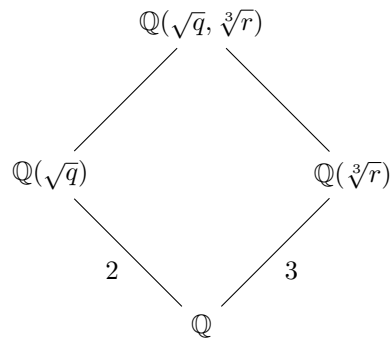
Before we attempt to approach the generalization, we should re-solve the original problem by Galois Theory to see whether the new theories really work and how brute calculation can be omitted.

3.1. The case $p = 7$ by Galois Theory

Problem. Prove that $\cos\dfrac{2\pi}{7}$ is not of the form $p + \sqrt{q} + \sqrt[3]{r}$, where p, q and r are rational numbers.

Proof. Suppose $\cos(2\pi/7) = p + \sqrt{q} + \sqrt[3]{r}$, where p, q and r are rational numbers. Then, $\cos(2\pi/7) \in \mathbb{Q}(\sqrt{q}, \sqrt[3]{r})$. Noting that , without loss of generality, we assume $\sqrt{q}$ and $\sqrt[3]{r}$ are not rational.

Consider the following field diagram,



Let $[\mathbb{Q}(\sqrt{q}, \sqrt[3]{r}) : \mathbb{Q}] = n$. Since $[\mathbb{Q}(\sqrt{q}) : \mathbb{Q}] = 2$ and $[\mathbb{Q}(\sqrt[3]{r}) : \mathbb{Q}] = 3$, both 2 and 3 divide n. Noting that

$$\mathbb{Q}(\sqrt{q}, \sqrt[3]{r}) = \{a_1 + a_2\sqrt{q} + a_3\sqrt[3]{r} + a_4\sqrt[3]{r^2} + a_5\sqrt{q}\sqrt[3]{r} + a_6\sqrt{q}\sqrt[3]{r^2} | a_i \in \mathbb{Q}\}$$

Therefore, $n \leq 6$. Thus, $n = 6$.

On the other hand, $\cos(2\pi/7) \in \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) = \mathbb{Q}(2\cos(2\pi/7))$. Consider the following field diagram,

$$\begin{array}{c} \mathbb{Q}(\zeta_7) \\ \Big| 2 \\ \mathbb{Q}(\zeta_7+\zeta_7^{-1}) = \mathbb{Q}(\cos(2\pi/7)) \\ \Big| 3 \\ \mathbb{Q} \end{array}$$

Since $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$ and $[\mathbb{Q}(\zeta_7) : \mathbb{Q}(\zeta_7 + \zeta_7^{-1})] = 2$, the Tower Law asserts that $[\mathbb{Q}(\zeta_7+\zeta_7^{-1}) : \mathbb{Q}] = 3$. Since $[\mathbb{Q}(\zeta_7+\zeta_7^{-1}) : \mathbb{Q}] \neq [\mathbb{Q}(\sqrt{q}) : \mathbb{Q}]$, $\mathbb{Q}(\zeta_7+\zeta_7^{-1}) \neq \mathbb{Q}(\sqrt{q})$.

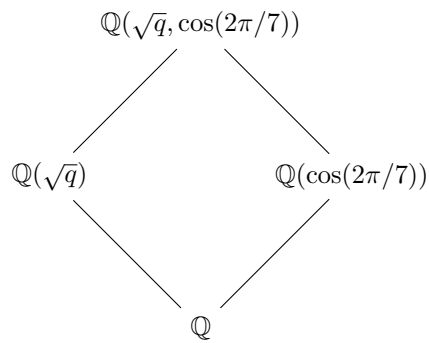
Then we consider $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \sqrt{q})$, using similar argument to the above, we have $[\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \sqrt{q}) : \mathbb{Q}] = 6$. Therefore, $[\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \sqrt{q}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{q}, \sqrt[3]{r} : \mathbb{Q}] = 6$.

Since $[\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \sqrt{q}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{q}, \sqrt[3]{r} : \mathbb{Q}]$ and we suppose that

$$\cos(2\pi/7) \in \mathbb{Q}(\sqrt{q}, \sqrt[3]{r}),$$

$\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \sqrt{q}) = \mathbb{Q}(\sqrt{q}, \sqrt[3]{r})$.

However, it is, indeed, impossible.



This is because, according to the above diagram, $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}$ is a Galois Extension, whereas $\mathbb{Q}(\sqrt{q}, \sqrt[3]{r})/\mathbb{Q}$ generally, is not Galois (except $q = -3$). Contradiction arises. [See reviewer's comment (7)]

If $q = -3$, then $Gal(\mathbb{Q}(\sqrt{-3}, \sqrt[3]{r})/\mathbb{Q}) \cong S_3$, which is not cyclic. However, $Gal(\mathbb{Q}(\zeta_7+\zeta_7^{-1})/\mathbb{Q})$ is cyclic as it is the subgroup of the cyclic group $Gal(\mathbb{Q}(\zeta_7)/\mathbb{Q})$. Thus, $q = -3$ is absurd. [See reviewer's comment (8)] □

Finally, we have tackled the problem successfully by Galois Theory, without any brute calculations. Therefore, it gives hope to prove our theorem. The next two lemmas are essential to our proof.

3.2. The First Lemma

We first recall the statement of the generalization we are working on.

Conjecture Let p be an odd prime, then $\cos\dfrac{2\pi}{p} = a_0 + a_1 + a_2 + \cdots + a_k$ for some $k \in \mathbb{Z}$, where $a_i = d_i^{1/p_i}$, $p_i = i$ th prime, $a_0, d_i \in \mathbb{Q}$, if and only if $p = 3$ or 5.

Suppose $\cos(2\pi/p) = a_0 + a_1 + a_2 + \cdots + a_k$. As $\cos(2\pi/p) \in \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, then $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is contained in $K = \mathbb{Q}(a_1, a_2, \ldots, a_k)$. Therefore, we can rephrase our conjecture in algebraic language, as following.

Lemma 29. *Let p be an odd prime. $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is contained in K if and only if $p = 3$ or 5.*

[See reviewer's comment (9)]

Proof. The sufficiency has been proved in Chapter 1. We now approach the necessity. Consider the following field diagram,

$$\begin{array}{c} K = \mathbb{Q}(a_1, a_2, \ldots, a_k) \\ | \\ \mathbb{Q}(\zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\cos(2\pi/p)) \\ | \\ \mathbb{Q} \end{array}$$

Let $J = \{i | a_i \notin \mathbb{Q}\}$. It is then obvious that $n = [K : Q] = \displaystyle\prod_{i \in J} p_i$, which is square-free. Therefore, by Tower Law, $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \dfrac{p-1}{2}$ is also square-free. Suppose q is a prime factor of $\dfrac{p-1}{2}$.

Since the Galois Group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is isomorphic to the multiplicative group $(\mathbb{Z}/\mathbb{Z}_p)^\times$, it is a cyclic group. Therefore, $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a cyclic extension. As $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is contained in $\mathbb{Q}(\zeta_p)$, $\mathbb{Q}(\zeta_p + \zeta_p^{-1})/\mathbb{Q}$ is also a cyclic extension. Therefore, according

to **Theorem 23**, for any prime q dividing $\dfrac{p-1}{2} = [\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}]$. there exists a field F contained in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ such that $[F : \mathbb{Q}] = q$. □

After this, we need another lemma, as shown in the next section.

3.3. The Second Lemma

Lemma 30. *If $F \subseteq \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \subseteq K$, then $F = \mathbb{Q}(a_i)$, where $p_i = q$.*

Proof. Recall the field diagram we have so far,

$$\begin{array}{c} K = \mathbb{Q}(a_1, a_2, \ldots, a_k) \\ | \\ \mathbb{Q}(\zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\cos(2\pi/p)) \\ | \\ F \\ | \\ \mathbb{Q} \end{array}$$

Consider the norm. By **Theorem 27**, we have $d_i^{[K:F]} = N_{K/F}(a_i^q) = (N_{K/F}(a_i))^q$. Therefore, $N_{K/F}(a_i) = d_i^{[K:F]/q} = (d_i^{1/q})^{[K:F]} = a_i^{n/q}$. As $\dfrac{n}{q} \in \mathbb{Z}$, we have $N_{K/F}(a_i) \in \mathbb{Q}(a_i)$.

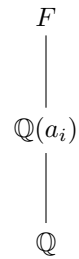
Since n is square-free and q is a prime, then $\left(\dfrac{n}{q}, q\right) = 1$. By **Bezout's lemma**, there exist integers x and y such that $\left(\dfrac{n}{q}\right)x + qy = 1$. Therefore,

$$a_i = a_i^{(n/q)x+qy} = (a_i^q)^y (a_i^{n/q})^x = (d_i^y)(N_{K/F}(a_i))^x$$

As $d_i \in \mathbb{Q}$, we have $a_i \in \mathbb{Q}(N_{K/F}(a_i))$.

As $a_i \in \mathbb{Q}(N_{K/F}(a_i))$ and $N_{K/F}(a_i) \in \mathbb{Q}(a_i)$, we have $\mathbb{Q}(N_{K/F}(a_i)) = \mathbb{Q}(a_i)$.

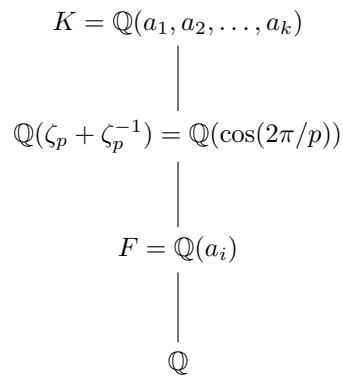
For all $\alpha \in K$, by **Theorem 24**, we have $\sigma_n(N_{K/F}(\alpha)) = N_{K/F}(\alpha)$, for all $\sigma_n \in Gal(K/F)$. [See reviewer's comment (10)] Thus, we have $N_{K/F}(\alpha) \in F$ for all $\alpha \in K$. Clearly that $a_i \in K$. Therefore, $N_{K/F}(a_i) \in F$.



Since $N_{K/F}(a_i) \in F$, $\mathbb{Q}(N_{K/F}(a_i))$ is contained in F, i.e. $\mathbb{Q}(a_i)$ is contained in F. Since q is a prime, degree consideration asserts that $\mathbb{Q}(a_i) = F$. [See reviewer's comment (11)] The second lemma is thus done. □

3.4. Proof of the generalization

Finally, we turn back to our First Lemma. [See reviewer's comment (12)] Renew the field diagram according to the information we have up to this moment,



Since $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a Galois and abelian extension, all its sub-extensions are Galois. It is clear that $\mathbb{Q}(\sqrt[q]{d_i})/\mathbb{Q}$ is a Galois Extension if and only if $q = 2$. The Second Lemma asserts that 2 is the only prime divisor of $\dfrac{p-1}{2}$. [See reviewer's comment (13)] As $\dfrac{p-1}{2}$ is square-free, $\dfrac{p-1}{2} = 2$ or $\dfrac{p-1}{2} = 1 \iff p = 3$ or 5. Noting that when $\dfrac{p-1}{2} = 1$, it means $\mathbb{Q}(\sqrt[q]{d_i}) = \mathbb{Q}$. Thus, the First Lemma is also done.

Our conjecture is a trivial corollary of the First Lemma. If $\cos(2\pi/p) \in \mathbb{Q}(\zeta_p + \zeta_p^{-1})$, then $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is contained in $K = \mathbb{Q}(a_1, a_2, \ldots, a_k)$, which happens if and only if $p = 3$ or 5. We are done!

4. Further investigation

After attaining the generalization, we want to investigate a bit further. Therefore, we modified the statement of our results. Instead of a prime denominator, we want to know what the situation becomes when it is replaced by a general natural number n.

Therefore, the problem now becomes what natural numbers n would satisfy

$$\cos(\frac{2\pi}{n}) = a_0 + a_1 + a_2 + \cdots + a_k$$

for some $k \in \mathbb{Z}$, where $a_i = d_i^{1/p_i}$, $p_i = i$th prime and $a_0, d_i \in \mathbb{Q}$?

Unfortunately, we failed to work it out because there are some difficulties to adopt our proof when we worked on composite denominator. However, we still state some particular results of the modified problem.

4.1. Hurdles for the general case: composite numbers n

[See reviewer's comment (14)]

We first recall the essential tricks we used when we proved the generalization with a prime denominator.

$$\begin{array}{c} K = \mathbb{Q}(a_1, a_2, \ldots, a_k) \\ | \\ \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos(2\pi/p)) \\ | \\ F = \mathbb{Q}(a_i) \\ | \\ \mathbb{Q} \end{array}$$

Referring back to the field diagram we had in Section 3.2, there are a few contributive and important steps, as follows.

1. $\dfrac{\phi(n)}{2}$ is square-free.
2. The existence of the subfield F. [See reviewer's comment (15)]

Therefore, we take these two points as the criteria that a general composite number n can satisfy our new conjecture.

To simplify the wording used in the following two sections, we would call those natural numbers n such that $\cos(\frac{2\pi}{n}) = a_0 + a_1 + a_2 + \cdots + a_k$ as "GOOD", otherwise as "BAD". For example, in previous chapter, we have proved that 3 and 5 are the only GOOD odd primes.

4.2. First Criterion: Square-free $\phi(n)/2$

If $\cos(2\pi/n) = a_0+a_1+a_2+\cdots+a_k$, then clearly $\cos(2\pi/n) \in K = \mathbb{Q}(a_1, a_2, \ldots, a_k)$.

$$\begin{array}{c} K = \mathbb{Q}(a_1, a_2, \ldots, a_k) \\ | \\ \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos(2\pi/n)) \\ | \\ \mathbb{Q} \end{array}$$

Since $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}] = \phi(n)/2$, the Tower Law asserts that $\phi(n)/2$ divides $[K : \mathbb{Q}]$. Since $[K : \mathbb{Q}]$ is square-free, $\phi(n)/2$ has to be square-free too. Therefore, those integers n which do not satisfy this condition would eventually become BAD.

The following is a result from Elementary Number Theory.

Theorem 31. *If n is a composite and $\phi(n)/2$ is square-free, then $n \in S = \{2^k p^i q^j : k \leq 3, i \leq 2, j \leq 2\}$, where p and q are distinct odd primes.*

Proof. Due to mutiplicativity of $\phi(n)$, we consider $\phi(p^\alpha)/2 = p^{\alpha-1}(p-1)/2$, where p is an odd prime. If $\phi(p^\alpha/2)$ is square-free, then obviously $\alpha - 1 < 2 \iff \alpha < 3$. [See reviewer's comment (16)] Since n is composite, $\alpha = 2$.

When $n = 2^k$, then $\phi(2^k)/2 = 2^{k-2}$. Using similar argument as above would assert that $k - 2 < 2 \iff k < 4$.

We recall the fact that if $d \mid n$, then $\phi(d) \mid \phi(n)$. Therefore, if n is divisible by three distinct prime factors p, q and r, then $\phi(n)$ is divisible by $\phi(pqr)$. But then $\phi(pqr)/2 = (p-1)(q-1)(r-1)/2$ is divisible by 4, implying n is BAD.

Thus, $\nu_p(n) \leq 2$, $\nu_2(n) \leq 3$ and n is divisible by at most 2 distinct prime factors. (Here $\nu_p(n)$ denotes the Legendre's valuation function, denoting the largest power of p dividing n.) In other words, $n \in S = \{2^k p^i q^j : k \leq 3, i \leq 2, j \leq 2\}$, where p and q are distinct primes. [See reviewer's comment (17)]

Indeed, we can reduce the size of the set S by observing that $\phi(4pq)/2 = (p-1)(q-1)$ and $\phi(8p^2)/2 = 2p(p-1)$, which are both divisible by 4. □

4.3. Example: the case $n = 15$

In this section, we would illustrate how to use the first criterion to prove that $n = 15$ is BAD, which is actually quite straightforward.

Problem. Prove that $\cos\dfrac{2\pi}{15}$ is not of the form $a_0 + a_1 + a_2 + \cdots + a_k$, where $k \in \mathbb{Z}$, $a_i = d_i^{1/p_i}$, $p_i = i$th prime and $a_0, d_i \in \mathbb{Q}$.

Proof. Similar to Section 3.1, we know that $\cos(2\pi/15) \in \mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1})$, and thus $\mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1})$ is contained in $K = Q(a_1, a_2, \ldots, a_k)$.

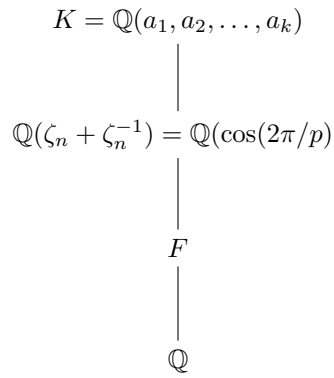
$$
\begin{array}{c}
K = \mathbb{Q}(a_1, a_2, \ldots, a_k) \\
\Big| \\
\mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}) = \mathbb{Q}(\cos(2\pi/15)) \\
\Big| \\
\mathbb{Q}
\end{array}
$$

Let $J = \{i | a_i \notin \mathbb{Q}\}$. It is then obvious that $n = [K : \mathbb{Q}] = \prod_{i \in J} p_i$, which is square-free. Therefore, by Tower Law, $[\mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}) : \mathbb{Q}]$ is also square-free. However, $[\mathbb{Q}(\zeta_{15} + \zeta_{15}^{-1}) : \mathbb{Q}] = \phi(15)/2 = 4 = 2^2$, contradiction arises. □

Performing similar proof, we can show that $16, 18, 20$ are also BAD since $\phi(16)/2 = 4$, $\phi(18)/2 = 9$ and $\phi(20)/2 = 4$. They are obviously not square-free.

4.4. Second Criterion: Cyclicity of $(\mathbb{Z}/n\mathbb{Z})^\times$

Another key step in our proof is to assert the existence of the field F in the following field diagram,



[See reviewer's comment (18)]

The existence of F is guaranteed by the cyclicity of the extension $\mathbb{Q}(\cos(2\pi/n))/\mathbb{Q}$, which is ensured further by the cyclicity of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is cyclic if and only if $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is cyclic. Since $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, we are sufficient to find what natural numbers n would satisfy that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if there is an element $\alpha \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $(\mathbb{Z}/n\mathbb{Z})^\times =< \alpha >$. In language of elementary number theory, it means that α is a primitive root modulo n.

Therefore, we can employ a classic result from elementary Number Theory concerning existence of primitive root.

Theorem 32. *(Primitive roots). There exists a primitive root modulo n if and only if $n = 1, 2, 4, p^k$, or $2p^k$, where p is an odd prime.*

However, the second criterion is relatively meaningless because the converse of **Theorem 23** may not be correct. But this criteria can be used to justify what composite numbers n are possible to be investigated along a similar proof given in Chapter 3. For example, when $n = 9$, $(\mathbb{Z}/9\mathbb{Z})^\times$ is cyclic. We can show that 9 is actually bad. We would illustrate it in the following section.

4.5. Example: the case $n = 9$

Problem. Prove that $\cos\dfrac{2\pi}{9}$ is not of the form $a_0 + a_1 + a_2 + \cdots + a_k$, where $k \in \mathbb{Z}$, $a_i = d_i^{1/p_i}$, $p_i = i$th prime and $a_0, d_i \in \mathbb{Q}$.

Proof. Suppose $\cos(2\pi/9) = a_0 + a_1 + a_2 + \cdots + a_k$, where p, q, r are rational numbers. Since $9 = 2 \times 3^2$, we know that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic. [See reviewer's comment (19)] Plus $\phi(9) = 6$, therefore 3 is a factor of $\phi(9)$. By **Lemma 29**, there exists a field F contained in $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ such that $[F : \mathbb{Q}] = 3$.

$$K = \mathbb{Q}(a_1, a_2, \ldots, a_k)$$
$$\mid$$
$$\mathbb{Q}(\zeta_9 + \zeta_9^{-1}) = \mathbb{Q}(\cos(2\pi/9))$$
$$\mid$$
$$F = \mathbb{Q}(a_2)$$
$$\mid$$
$$\mathbb{Q}$$

Since $p_i = 3$, we have $i = 2$. By **Lemma 30**, $F = \mathbb{Q}(a_2)$. Clearly $\mathbb{Q}(\sqrt[3]{d_2})/\mathbb{Q}$ is not Galois, contradiction arises. □

In fact, the case of $n = 14$ and $n = 18$ can be tackled similarly since $(\mathbb{Z}/14\mathbb{Z})^\times$ and $(\mathbb{Z}/18\mathbb{Z})^\times$ are both cyclic.

4.6. Summary

In Chapter 3, we have proved that 3 and 5 are the only GOOD odd primes. Although we fail to generalize our theorem for the composite cases, we have given two criteria to classify some composite numbers to be GOOD or BAD. However, for those composites which cannot be classified by these two criteria, we have to give independent proof. To end our project, we list out all the GOOD and BAD natural numbers up to 20.

All the BAD numbers within this range are $7, 9, 11, 13, 14, 15, 16, 17, 18, 19, 20$. The rest are all GOOD, as shown in following,

$$n = 1, \cos\left(\frac{2\pi}{1}\right) = 1;$$
$$n = 2, \cos\left(\frac{2\pi}{2}\right) = -1;$$
$$n = 3, \cos\left(\frac{2\pi}{3}\right) = -\frac{1}{2};$$
$$n = 4, \cos\left(\frac{2\pi}{4}\right) = 0;$$

$$n = 5, \cos\left(\frac{2\pi}{5}\right) = -\frac{1}{4} + \sqrt{\frac{5}{16}};$$
$$n = 6, \cos\left(\frac{2\pi}{6}\right) = -\frac{1}{2};$$
$$n = 8, \cos\left(\frac{2\pi}{8}\right) = \sqrt{\frac{1}{2}};$$
$$n = 10, \cos\left(\frac{2\pi}{10}\right) = \frac{1+\sqrt{5}}{4};$$
$$n = 12, \cos\left(\frac{2\pi}{12}\right) = \sqrt{\frac{3}{4}}.$$

REFERENCES

[1] Michael Artin, *Algebra*, Pearson Education, 1991.
[2] John B. Fraleigh, *A First Course in Abstract Algebra*, 7th. ed., Addison Wesley.
[3] Kenneth Ireland, Michael Rosen, *A Classical Introduction to Modern Number Theory*, 2nd. ed., Springer-Verlag, 1990.
[4] Patrick Morandi, *Field and Galois Theory*, Springer-Verlag.
[5] Ivan Niven, Herbert S.Zuckerman, Hugh L.Montgomery, *An introduction to the Theory of Numbers*, 5th ed. John Wiley and Sons, 1991.
[6] Steven Roman, *Field Theory*, Springer-Verlag.
[7] Joseph Rotman, *Galois Theory*, 2nd. ed., Springer-Verlag.

Reviewer's Comments

The paper under review addresses the following problem which was inspired by one from a math competition: determine the odd primes p such that $\cos\frac{2\pi}{p}$ can be expressed as a sum $\sum_{i=1}^{k} a_i$, where a_i are of the form $d_i^{\frac{1}{p_i}}$ with p_i being the i-th prime and d_i rational. The authors first set the scene by stating the original problem of showing that $\cos\frac{2\pi}{7}$ is not of the desired form, reproducing a proof by Prof. Kin Yin Li which involves high school algebra, and pointing out the difficulties of generalizing the elementary techniques employed in the original proof to the case $p = 11$. Prompted by their advisor, the authors tackle the problem using Galois theory instead, which is reviewed in Chapter 2 of the paper. Their solution, which is the content of Chapter 3, makes ingenious use of the properties of Galois (in particular, cyclotomic) extensions and their degrees. In particular, they show that, if $\cos\frac{2\pi}{p}$ is expressible in the desired form, then

1. $\mathbb{Q}(\cos\frac{2\pi}{p}) \subset \mathbb{Q}(a_1, \cdots, a_k)$, and if q is a prime divisor of $\frac{p-1}{2}$, which is shown to be square-free, then there is a field $F \subseteq \mathbb{Q}(\cos\frac{2\pi}{p})$ such that $[F : \mathbb{Q}] = q$,
2. $F = \mathbb{Q}(a_i)$ for some $1 \leq i \leq n$ if $F \subseteq \mathbb{Q}(\cos\frac{2\pi}{p})$, and
3. $\mathbb{Q}(\cos\frac{2\pi}{p})$ and hence F are Galois extensions over $\mathbb{Q}$.

They also observe that $\mathbb{Q}(a_i)$ is Galois over $\mathbb{Q}$ if and only if $p_i = 2$. As a result, they prove that only when $p = 3$ or 5 can $\cos\frac{2\pi}{p}$ be expressed in the desired form. In the last chapter of their paper they explore the more general case where p is replaced by a general natural number n, and manage to give partial results by carrying over the salient points in their proof for the prime case.

In general, the paper is clearly written and well-organized. The authors are able to formulate their problem and goal precisely, extract the relevant ingredients in Galois theory they need and give a neat proof of the problem. However, the paper is still riddled with some issues in presentation and typing, as well as grammatical mistakes, which are listed below.

1. The reviewer has comments on the wordings, which have been amended in this paper.
2. Though references are listed in the end of the paper, the authors should also explicitly cite the references in the body of the paper wherever appropriate.
3. It is better to say 'give its statement' rather than 'state its statement'.
4. 'functions' should be changed to 'automorphisms'. '$\sigma_i(\alpha) = \alpha^i$' should be changed to '$\sigma_i(\zeta_n) = \zeta_n^i$'.
5. The Euler totient function ϕ should be defined before stating Theorem 20.
6. It is a good idea to first define normal extension, and state the first sentence of Theorem 23 ('A finite normal extension...a cyclic group') separately as the definition of cyclic extension before stating Theorem 23.

7. It is better to say something along the line '$\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \sqrt{q})/\mathbb{Q}$ is a Galois extension because both $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$ are, whereas...'. 'Contradiction arises' should be deleted because at this point, the exceptional case $q = -3$ has not been discussed and so we have not reached an absolute contradiction. Only state this at the end of the proof.
8. It is not obvious to the reviewer why the first two sentences contradict each other. The reviewer thinks it is better to replace the second sentence with something along the line 'However, $\mathrm{Gal}(\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \sqrt{-3})/\mathbb{Q}) \cong \mathbb{Z}_6$'.
9. Lemma 29 should be stated as a theorem (say, Theorem 29) instead because it is a rephrasing of the main result of the paper. As the proof following the Lemma 29 is not actually its proof, it is better to state the following as a lemma immediately proceeding the proof and after the rephrasing of the main result.

   Lemma If $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is contained in K, then
   (a) $\frac{p-1}{2}$ is square-free, and
   (b) for any prime q which divides $\frac{p-1}{2}$, there exists a field $F \subseteq \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ such that $[F : \mathbb{Q}] = q$.
10. 'by Theorem 24' should be changed to 'by an easy generalization of Theorem 28'. In fact what follows is obviously derived from a generalization of Theorem 28 instead of Theorem 24 (not exactly Theorem 28 because it is about the case of cyclotomic extensions only, whereas in the present situation K may not be a cyclotomic extension). Alternatively, Theorem 28 can be stated in its more general form which deals with any field extension, and in this way 'by Theorem 24' can be changed to 'by Theorem 28'.
11. Change 'degree consideration asserts that...' to 'by degree consideration, we have that...'
12. Change 'First Lemma' to 'Theorem 29'.
13. Change 'The Second Lemma' to 'The first two lemmata'.
14. It is confusing to use n to denote, on the one hand, the denominator as in $\cos \frac{2\pi}{n}$ and, on the other hand, the degree $[K : \mathbb{Q}] = \prod_{i \in J} p_i$ as in the proof of Lemma 29. Use another alphabet to denote the denominator.
15. It is a good idea to point out that the first criterion is a necessary condition for n to be a good number. The second criterion is vague to the reviewer: what kind of subfield is F? Is it of the form $\mathbb{Q}(a_i)$ as in the second lemma, or does it satisfy $[F : \mathbb{Q}]$ is a prime as in the first lemma? The reviewer believes the authors mean that F is of the form specified in the second lemma. Besides it is confusing to see that this second criterion is not the same as the condition of cyclicity of $(\mathbb{Z}/n\mathbb{Z})^\times$ discussed in Section 4.4, the title of which claims that the latter condition is the second criterion.
16. '$\phi(p^\alpha/2)$' should be changed to '$\phi(p^\alpha)/2$'.
17. Insert 'odd' between 'distinct' and 'prime'.
18. The tower diagram: change 'p' to 'n' or another alphabet.
19. What are p, q and r? The reviewer thinks the phrase 'where p, q, r are rational numbers' should be deleted. Change '$9 = 2 \times 3^2$' to '$9 = 3^2$'.