The Algebraic Degree of $\cos(\frac{a\pi}{m})$
An Exposition by
William Gasarch
Auguste Gezalyan

1 Introduction

The following are well known: (a) $\cos(\pi/1) = -1$, (b) $\cos(\pi/2) = 0$, (c) $\cos(\pi/3) = \frac{1}{2}$, (d) $\cos(\pi/4) = \frac{\sqrt{2}}{2}$, and (e) $\cos(\pi/6) = \frac{\sqrt{3}}{2}$. Note that $\cos(\pi/5)$ is missing. In Harold Boas's paper [1] he shows that $\cos(\pi/5) = \frac{1+\sqrt{5}}{4}$, which is half the golden ratio. Note that all of these numbers are algebraic.

Are numbers of the form $\cos(a\pi/b)$ with $a, b \in \mathsf{N}$ always algebraic? Yes. This is well known. Indeed, more is known. We need two defintions to state what is known.

Def 1.1 α is an *algebraic number* if there exists a polynomial $p(x) \in \mathsf{Z}[x]$ such that $p(\alpha) = 0$. The *degree of* α is the degree of the least-degree such polynomial. We denote this $\deg(\alpha)$.

Def 1.2 $\phi(n)$ is the number of elements of $\{1, \ldots, n\}$ that are relatively prime to n. It is often called the *Euler Totient Function*.

We have been told that the following are well known:

1. If $a, b \in \mathsf{N}$, $\gcd(a, b) = 1$, and a is odd, then $\deg(\cos(a\pi/b)) = \phi(2b)/2$
2. If $a, b \in \mathsf{N}$, $\gcd(a, b) = 1$, and a is even, then $\deg\cos((a\pi/b)) = \phi(b)/2$.

Despite being "well known" we have not been able to find a proof on the web. (If a proof is not on the web then has the theorem been proven?) We remedy this situation by giving a proof. We try to prove all needed lemmas, even if they are also "well known." The proof is not original to us. Most of this paper is standard material (though put together for this proof). The key steps that are not standard material, Lemma 4.1 and Theorem 4.2, were given to us by Larry Washington.

2 Degrees of Extensions and Degrees of Algebraic Numbers

Def 2.1

1. A *Number Field* is a subset of C that is a field.

2. Let E and F be number fields such that $F \subseteq E$. It is easy to see that E is a vector space over F. The *degree of E over F*, denoted $[E : F]$, is the dimension of E viewed as a vector space over F. We will only deal with the case where $[E : F]$ is finite.

We relate the degree of a field extension with the degree of an algebraic number.

Lemma 2.2 *Let α be an algebraic number.*

1. $[\mathsf{Q}(\alpha) : \mathsf{Q}] \leq \deg(\alpha)$.
2. $\deg(\alpha) \leq \mathsf{Q}(\alpha) : \mathsf{Q}]$.
3. $[\mathsf{Q}(\alpha) : \mathsf{Q}] = \deg(\alpha)$. *This follows from Parts 1,2.*

Proof:
1) Assume $\deg(\alpha) = d$. Then there exists $a_0, \ldots, a_d \in \mathsf{Z}$ such that $\sum_{i=0}^{d} a_i \alpha^i = 0$. We rewrite this as $\alpha^d = -\frac{1}{a_d} \sum_{i=0}^{d-1} a_i \alpha^i$.

We show that $\{1, \alpha, \ldots, \alpha^{d-1}\}$ is a basis for $\mathsf{Q}(\alpha)$ over Q.
Span Since $\alpha^d = -\frac{1}{a_d} \sum_{i=0}^{d-1} a_i \alpha^i$, $\mathsf{Q}(\alpha)$ is in the span over Q of $\{1, \alpha, \ldots, \alpha^{d-1}\}$.
Linearly Independent If there exists $b_0, \ldots, b_{d-1} \in \mathsf{Q}$ such that $\sum_{i=0}^{d-1} b_i \alpha^i = 0$ then, since $\deg(\alpha) = d$, $b_0 = \cdots = b_{d-1} = 0$.

2) Assume $[\mathsf{Q}(\alpha) : \mathsf{Q}] = d$. Then the set $\{1, \alpha, \alpha^2, \ldots, \alpha^d\}$ is linearly dependent over Q. Hence there exists $a_0, \ldots, a_d \in \mathsf{Q}$, not all 0, such that

$$\sum_{i=0}^{d} a_i \alpha^i = 0$$

Clear fractions to obtain a polynomial $p(x) \in \mathsf{Z}[x]$ of degree $\leq d$ such that $p(\alpha) = 0$. Hence $\deg(\alpha) \leq d = [\mathsf{Q}(\alpha) : \mathsf{Q}] = d$. ∎

Lemma 2.3 *Let K, L, M be number fields such that $K \subseteq L \subseteq M$. Then*

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

Proof: Let d, e be such that $[L : K] = d$ and $[M : L] = e$.
Let the basis for K over L be $\{u_1, \ldots, u_d\}$.
Let the basis for L over M be $\{w_1, \ldots, w_e\}$.
We show that $\{u_i w_j : 1 \leq i \leq d, 1 \leq j \leq e\}$ is a basis for K over M.
Let $x \in K$. Then there exists $a_1, \ldots, a_d \in L$ such that

$$x = \sum_{i=1}^{d} a_i u_i.$$

Express each a_i as a linear combination of the w_j's over M to get x as a linear combination of $\{u_i w_j : 1 \leq i \leq d, 1 \leq j \leq e\}$ over M.

We now check that the basis is linearly independent of M. Assume that there exists $b_{m,n}$ such that

$$\sum_{n=1}^{e} \sum_{m=1}^{d} b_{m,n}(u_m w_n) = 0$$

Then

$$\sum_{n=1}^{e} (\sum_{m=1}^{d} b_{m,n} u_m) w_n = 0$$

Since $w_1, \ldots, w_e$ is a basis of L over M we have that

$$(\forall n)[\sum_{m=1}^{d} b_{m,n} u_m = 0]$$

Since $u_1, \ldots, u_d$ is a basis for K over L we have that each $b_{m,n} = 0$.

∎

Lemma 2.4 *Let α be an algebraic number. If α is the root of an irreducible polynomial $p(x) \in \mathsf{Z}[x]$ of degree d then* $\deg(\alpha) = d$.

Proof: Assume, by way of contradiction, that $\deg(\alpha) = e < d$. Then α is the root of an irreducible polynomial $q(x) \in \mathsf{Z}[x]$ of degree e. Since $p(x)$ and $q(x)$ are both irreducible, $\gcd(p(x), q(x)) = 1$. Hence by the Euclideian algorithm there exists $a(x), b(x) \in \mathsf{Z}[x]$ such that

$$a(x)p(x) + b(x)q(x) = 1.$$

Plug in $x = \alpha$ into this to get

$$a(\alpha)p(\alpha) + b(\alpha)q(\alpha) = 1.$$

Since $p(\alpha) = 0$ and $q(\alpha) = 0$ we get $0 = 1$, a contradiction. ∎

3 Cyclotomic Polynomials

Def 3.1 Let $n \in \mathsf{N}$. The *nth Cyclotomic Polynomial* is

$$\Phi_n(x) = \prod_{1 \leq k \leq n, \gcd(k,n)=1} (x - e^{2k\pi i/n}).$$

We will show that $\Phi_n(x) \in \mathsf{Z}[x]$.

Lemma 3.2 *Let $n \in \mathsf{N}$.*

1. *If $n \geq 2$ then $\sum_{1 \leq k \leq n, \gcd(k,n)=1} k \equiv 0 \pmod{n}$.*
2. *If $n \geq 2$ then $\Phi_n(x)$ has constant term 1.*
3. *If $n \geq 1$ then $\Phi_n(x)$ has constant term ± 1.*
4. *The product of any number of $\Phi_d(x)$'s has constant term ± 1. (This follows from Parts 2,3.)*

Proof:
1) If $\gcd(k,n) = 1$ then $\gcd(n-k,n) = 1$. Hence in the sum pair up the k's and $n-k$'s to get a multiple of n.
2) The constant term of $\Phi_n(x)$ is

$$\prod_{1 \leq k \leq n, \gcd(k,n)=1} e^{2k\pi i/n} = e^{\frac{2\pi i}{n} \sum_{1 \leq k \leq n, \gcd(k,n)=1} k}.$$

By Part 1 the sum is $\equiv 0 \pmod{n}$. Hence the exponent is an integer multiple of $2\pi i$. So the expression is 1.
3) Part 2 shows that if $n \geq 2$ then $\Phi_n(x)$ has constant term 1. Since $\Phi_1(x) = x - 1$, we are done. ∎

Lemma 3.3 *Let $n \geq 1$. Assume that*

$$(x^n - 1) = (\sum_{i=1}^{p} a_i x_i)(\sum_{j=1}^{q} b_j x^j)$$

where $a_p = \pm 1$ and $(\forall i)[a_i \in \mathsf{Z}]$. Then $(\forall j)[b_j \in \mathsf{Z}]$.

Proof: We proof this by backward induction.
Base Case $j = q$: Since $a_p b_q = 1$ and $a_p = \pm 1$, $b_q = a_p = \pm 1 \in \mathsf{Z}$.
Ind Hyp: Assume $b_q, b_{q-1}, \ldots, b_{r+1} \in \mathsf{Z}$.
Ind Step: Since $0 \leq r \leq q-1$, $1 \leq p \leq p+r \leq p+q-1 \leq n-1$. So $1 \leq p+r \leq n-1$. Hence the coefficient of x^{p+r} is 0. Therefore

$$a_p b_r + a_{p-1} b_{r+1} + \cdots + a_{p+r} b_q = 0.$$

$$b_r = -\frac{a_{p-1} b_{r+1} + \cdots + a_{p+r} b_q}{a_p}.$$

The numerator is in Z by the Ind. Hyp. The denominator is ± 1 by hypothesis. So $b_r \in \mathsf{Z}$.
∎

Lemma 3.4 *Let $n \geq 1$. Then*

$$(x^n - 1) = \prod_{d|n} \Phi_d(x).$$

Proof: Clearly every root of $\prod_{d|n} \Phi_d(x)$ is a root of $x^n - 1$.

We show that every root of $x^n - 1$ is a root of $\prod_{d|n} \Phi_d(x)$.

The roots of $x^n - 1$ are $\{e^{2k\pi i/n} : 1 \leq k \leq n\}$. Let $e^{2k\pi i/n}$ be a root. Let $2k\pi i/n = a\pi i/d$ where $\gcd(a, d) = 1$. Note that d divides n and $e^{a\pi i/d}$ is a root of $\Phi_d(x)$. Hence $e^{2k\pi i/n}$ is a root of $\prod_{d|n} \Phi_d(x)$. ∎

Theorem 3.5 *For all $n \geq 1$, $\Phi_n(x) \in \mathsf{Z}[x]$.*

Proof: We prove this by induction on n.

Base Case $\Phi_1(x) = x - 1 \in \mathsf{Z}[x]$.

Ind Hyp For all $d \leq n - 1$, $\Phi_d(x) \in \mathsf{Z}[x]$.

Ind Step By Lemma 3.4

$$(x^n - 1) = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \prod_{d|n, d<n} \Phi_d(x).$$

By the Ind Hyp $\prod_{d|n,d<n} \Phi_d(x) \in \mathsf{Z}[x]$. By Lemma 3.2.d the constant term of $\prod_{d|n,d<n} \Phi_d(x)$ is ± 1. By Lemma 3.3 $\Phi_n(x) \in \mathsf{Z}[x]$. ∎

Lemma 3.6 *Let $n, k \in \mathsf{N}$ with $\gcd(k, n) = 1$.*

1. *For all n, $\Phi_n(x)$ is irreducible.*
2. *$\deg(e^{2\pi ik/n}) = \phi(n)$. (This follows from $e^{2\pi ik/n}$ being a root of $\Phi_n(x)$, $\Phi_n(x)$ being irreducible, $\Phi_n(x)$ having degree $\phi(n)$, and Lemma 2.4.)*
3. *$[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}] = \phi(n)$. (This follows from Part 2 and Lemma 2.2.)*

Proof:
1) FILL IN LATER.
∎

4 The Degree of $\cos(a\pi/b)$

Lemma 4.1 *Let $n, k \in \mathsf{N}$ with $\gcd(k,n) = 1$. $[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}(\cos(2\pi k/n)] = 2$.*

Proof: This proof is in two parts. We first show that $[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}(\cos(2\pi k/n)] \geq 2$. We then show that $[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}(\cos(2\pi k/n)] \leq 2$.
a) We first show that $[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}(\cos(2\pi k/n)] \geq 2$. Assume, by way of contradiction, that $[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}(\cos(2\pi k/n)] = 1$. Let the basis be $\{v\}$ where $v \in \mathsf{Q}(e^{2\pi ik/n})$. Since $Q(e^{2\pi ik/n})$ has elements of $\mathsf{C} - \mathsf{R}$ and $\mathsf{Q}(\cos(2\pi k/n) \subseteq \mathsf{R}$, $v \in \mathsf{C} - \mathsf{R}$.

Since $e^{2\pi ik/n} \in \mathsf{Q}(e^{2\pi ik/n})$ there must be $a \in \mathsf{Q}(\cos(2\pi k/n)$ such that $e^{2\pi ik/n} = av$. Note that $a \in \mathsf{R}$.

Since $e^{-2\pi ik/n} \in \mathsf{Q}(e^{2\pi ik/n})$ there must be $b \in \mathsf{Q}(\cos(2\pi k/n)$ such that $e^{-2\pi ik/n} = bv$. Note that $b \in \mathsf{R}$.

Note that

- $e^{2\pi i/n} + e^{-2\pi i/n} = av + bv = (a+b)v$.
- $e^{2\pi i/n} + e^{-2\pi i/n} = \frac{\cos(2\pi/n)}{2}$.

Hence

$$(a+b)v = \frac{\cos(2\pi/n)}{2}.$$

$$v = \frac{\cos(2\pi/n}{2(a+b)} \in \mathsf{R}.$$

This contradicts $v \notin \mathsf{R}$.
b) Note that $e^{2\pi ik/n}$ is a root of the quadratic equation

$$X^2 - 2\cos(2\pi k/n)X + 1 = 0.$$

One can use this to show that $\{1, e^{2\pi ik/n}\}$ spans $\mathsf{Q}(e^{2\pi ik/n})$ over $\mathsf{Q}(\cos(2\pi k/n)]$. (This is similar to the proof of Lemma 2.2.1.) ∎

Theorem 4.2

1. *Let $n, k \in \mathsf{N}$ with $\gcd(k,n) = 1$. Then $\deg(\cos(2\pi k/n) = \phi(n)/2$.*
2. *If $a, b \in \mathsf{N}$, $\gcd(a,b) = 1$, and a is odd then $\deg(\cos(a\pi/b)) = \phi(2b)/2$.*
3. *If $a, b \in \mathsf{N}$, $\gcd(a,b) = 1$, and a is even then $\deg\cos((a\pi/b)) = \phi(b)/2$.*

Proof:
1) By Lemma 2.3

$$[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}] = [\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}(\cos(2\pi k/n)][\mathsf{Q}(\cos(2\pi k/n) : \mathsf{Q}].$$

By Lemma 3.6

$$[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}] = \phi(n).$$

By Lemma 4.1

$$[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}(\cos(2\pi k/n)] = 2.$$

Hence

$$[\mathsf{Q}(\cos(2\pi k/n) : \mathsf{Q}] = \frac{[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}]}{[\mathsf{Q}(e^{2\pi ik/n}) : \mathsf{Q}(\cos(2\pi k/n)]} = \phi(n)/2.$$

By Lemma 2.2 $\deg(\cos(2\pi k/n) = \phi(n)/2$.
2) $\deg(\cos(a\pi/b)) = \deg(\cos(2a\pi/2b))$. Since a is odd and $\gcd(a, b) = 1$, $\gcd(a, 2b) = 1$. By Part 1 $\deg(\cos(2a\pi/2b) = \phi(2b)/2$. ∎

3) $\deg(\cos(a\pi/b)) = \deg(\cos(2(a/2)\pi/b)$. Since a is even , $a/2 \in \mathsf{N}$. Since $\gcd(a, b) = 1$, $\gcd(a/2, b) = 1$. By Part 1 $\deg(\cos(2(a/2)\pi/b) = \phi(b)/2$.

References

[1] H. Boas. The oldest trig in the book. *College Mathematics Journal*, 50(1):9–20, 2019.