Part of Paper that Use Field Theory
by

William Gasarch
Auguste Gezalyan

1 $\deg(\cos(v\pi/n))$ & $\deg(\sin(v\pi/n))$: Field Theory

1.1 Background Needed

We state well known facts from field theory and use them to prove our results. All fields are subsets of C.

Definition 1.1 Let F and E be fields. E is *a field extension of* F if

- $\mathsf{F} \subseteq \mathsf{E}$.
- The operations $+, \times$ in F are $+, \times$ in E restricted to F.

Fact 1.2

1. *If* E *is a field extension of* F *then* E *is a vector space over* F*. We denote the dimension of this vector space by* $[\mathsf{E} : \mathsf{F}]$*.*
2. *If* D *is a field extension of* E *and* E *is a field extension of* F *then* $[\mathsf{D} : \mathsf{F}] = [\mathsf{D} : \mathsf{E}][\mathsf{E} : \mathsf{F}]$*.*

Definition 1.3 Let $\mathsf{F} \subseteq \mathsf{C}$ be a field and let $\alpha \in \mathsf{C} - \mathsf{F}$.

$$\mathsf{F}(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)} : p, q \in \mathsf{F}[x] \text{ and } q(\alpha) \neq 0 \right\}.$$

Definition 1.4 Let E be a field extension of F. Let $\alpha \in \mathsf{E}$. *The degree of* α over F is the smallest $d \in \mathsf{N}$ such that α is the root of a degree-d polynomial in $\mathsf{F}[x]$. We denote this by $\deg_{\mathsf{F}}(\alpha)$. If $\mathsf{F} = \mathsf{Q}$ then we just use deg which matches the definition of deg we have been using.

Fact 1.5 $\mathsf{F}(\alpha)$ *is a field extension of* F *and* $[\mathsf{F}(\alpha) : \mathsf{F}] = \deg_{\mathsf{F}}(\alpha)$*.*

Proof:
Clearly $\mathsf{F}(\alpha)$ is a field extension of F.
Let $\deg_F(\alpha) = d$.
We show that The set $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ forms a basis for $[\mathsf{F}(\alpha) : \mathsf{F}]$.

- Every element of $\mathsf{F}(\alpha)$ is a polynomial in α with coefficients in F. Since $\deg_F(\alpha) = d$, the polynomials can be made to be of degree $\le d$.
- Let $a_0, \ldots, a_{d-1} \in \mathsf{F}$ be such that $\sum_{i=0}^{d-1} a_i \alpha^i = 0$. Since $\deg_F(\alpha) = d$, all of the a_i are 0.

▮

Note 1.6 Lets say you prove that $[\mathsf{Q}(\alpha) : \mathsf{Q}] = d$, so $\deg(\alpha) = d$. Can Fact 1.5 help *find* a polynomial of degree d that has α as a root. No. All you find out is that $\{1, \alpha, \ldots, \alpha^d\}$ is linearly dependent over Q, hence *there exists* such a polynomial. But the proof of Fact 1.5 does not say how to *find* the polynomial.

BEGINNING OF COMMENTS TO AUGUSTE

(I DO NOT KNOW IF THE NOTE ABOVE IS CORRECT.)

We just proved $[\mathsf{F}(\alpha) : F] = \deg_{\mathsf{F}}(\alpha)]$ but for us for now lets just consider $[\mathsf{Q}(\alpha) : F] = \deg_{\mathsf{Q}}(\alpha)]$

1) The proof is contructive in one direction: Given α we can get a basis, namely

$$\{1, \alpha, \ldots, \alpha^{d-1}\}.$$

(Note- not clear what *given* means since α is irrational.)

2) Can the following be done: Given α and d where one is told that there is a poly $p \in \mathsf{Z}[x]$ of degree d that has α as a root, find that poly?

Actually the answer is yes for a stupid way: enumerate all polys and test each one until you find one. But even this is not really right since α is irrational so this would need perfect real arithmetic.

It may be that for our case of $\cos(v\pi/n)$ this can be dealt with.

So the question is, is there a SANE algorithm.

3) In Lemma 1.10 below we prove the following:

——-

Let $1 \le v \le n-1$ be such that $\gcd(v, n) = 1$.

$[\mathsf{Q}(\cos(2\pi v/n)) : \mathsf{Q}] = \phi(n)/2$.

Hence $\deg(\cos(2\pi v/n)) = \phi(n)/2$.

————-

SO here are my questions:

From the proof of this one can one, given v, n (that is an input you CAN be given) find poly $p \in \mathsf{Z}[x]$ of degree $\phi(n)/2$ that has α as a root.

If so, then (a) is the algorithm SANE, and (b) does the algorithm need perfect arithmetic for reals?

Much like Maya's personal statement, I don't want our final paper to dwell on this point. I want to BRIEFLY talk about how the proof using Field theory can or cannot be used to

find he poly, and if yes then does or does not use real arithmetic. I will then also state this as probably one of the CONS when I discuss PROS and CONS early in the paper
END OF COMMENTS TO AUGUSTE

Notation 1.7 $\zeta_n = e^{2\pi i/n}$. (ζ is the Greek letter zeta.)

Definition 1.8 Let $n \in \mathsf{N}$. α is an *nth root of unity* if $\alpha^n = 1$. α is a *primitive root of unity* if (1) $\alpha^n = 1$, and (2) for every $n' < n$, $\alpha^{n'} \neq 1$.

Fact 1.9

1. *There are n nth roots of unity:* $\zeta_n^1, \ldots, \zeta_n^n$.
2. *There are* $\phi(n)$ *primitive nth roots of unity:* $\{\zeta_n^v\colon \gcd(v,n) = 1\}$.
3. *If* α *is a primitive nth root of unity then* $\deg(\alpha) = \phi(n)$.

1.2 deg (cos ($v\pi/n$)) Via Field Theory

Lemma 1.10 *Let* $1 \le v \le n-1$ *be such that* $\gcd(v,n) = 1$.

1. $[\mathsf{Q}(\zeta_n^v) : \mathsf{Q}] = \phi(n)$.
2. *If* $n \ge 3$ *then* $[\mathsf{Q}(\zeta_n^v) : \mathsf{Q}(\cos(2\pi v/n))] = 2$.
3. $[\mathsf{Q}(\cos(2\pi v/n)) : \mathsf{Q}] = \phi(n)/2$.
4. $\deg(\cos(2\pi v/n)) = \phi(n)/2$.

Proof:
1) $[\mathsf{Q}(\zeta_n^v) : \mathsf{Q}] = \phi(n)$ follows from Fact 1.5 and Fact 1.9.3.

2) $[\mathsf{Q}(\zeta_n^v) : \mathsf{Q}(\cos(2\pi v/n))] = \deg_{\mathsf{Q}(\cos(2\pi v/n))}(\zeta_n^v)$. Hence we need to find $\deg_{\mathsf{Q}(\cos(2\pi v/n))}(\zeta_n^v)$.
$\deg_{\mathsf{Q}(\cos(2\pi v/n))}(\zeta_n^v) \le 2$ since ζ_n^v is a root of $x^2 - 2\cos(2v\pi/n)x + 1$.
$\deg_{\mathsf{Q}(\cos(2\pi v/n))}(\zeta_n^v) \ge 2$:

Assume, by way of contradiction, that ζ_n^v is the root of a linear polynomial with coefficients in $\mathsf{Q}(\cos(2\pi v/n))$. Then $\zeta_n^v \in \mathsf{Q}(\cos(2\pi v/n))$ and hence $\zeta_n^v \in \mathsf{R}$. Since $n \ge 3$, $\zeta_n \in \mathsf{C} - \mathsf{R}$. This is a contradiction.

3) By Fact 1.2.2

$$[\mathsf{Q}(\zeta_n^v) : \mathsf{Q}] = [\mathsf{Q}(\zeta_n^v) : \mathsf{Q}(\cos(2\pi v/n))][\mathsf{Q}(\cos(2\pi v/n)) : \mathsf{Q}]$$

By Part 1 and Part 2 we have

$$\phi(n) = 2[\mathsf{Q}(\cos(2\pi v/n)) : \mathsf{Q}].$$

Hence $[\mathsf{Q}(\cos(2\pi v/n)) : \mathsf{Q}] = \phi(n)/2$.

4) By Part 3 $[\mathsf{Q}(\cos(2\pi v/n)) : \mathsf{Q}] = \phi(n)/2$. By Fact 1.5

$$\deg(\cos(2\pi v/n))) = [\mathsf{Q}(\cos(2\pi v/n)) : \mathsf{Q}] = \phi(n)/2.$$

▮

Theorem 1.11 *Let* $1 \le v \le n$ *such that* $\gcd(v, n) = 1$.

1. *If n is odd then* $\deg(\cos(v\pi/n)) = \phi(n)/2$.
2. *If n is even then* $\deg(\cos(v\pi/n)) = \phi(n)$.

Proof:
1) n **is odd.** There are two cases

Case 0: v is even. Then $v = 2v'$. Hence $\deg(\cos(v\pi/n)) = \deg(\cos(2v'\pi/n))$.

Since $\gcd(v, n) = 1$, $\gcd(v', n) = 1$. Hence, by Lemma 1.10.4, $\deg(\cos(2v'\pi/n)) = \phi(n)/2$, so $\deg(\cos(v\pi/n)) = \phi(n)/2$.

Case 1: v is odd. Note that $\deg(\cos(v\pi/n)) = \deg(\cos(2v\pi/2n))$.

Since v is odd and $\gcd(v, n) = 1$, $\gcd(v, 2n) = 1$. Hence, by Lemma 1.10.4, $\deg(\cos(2v\pi/2n)) = \phi(2n)/2$. Since n is odd, $\phi(2n) = \phi(n)$ so $\deg(\cos(v\pi/n)) = \phi(n)/2$.

2) n **is even.** Note that $\deg(\cos(v\pi/n)) = \deg(\cos(2v\pi/2n))$.

Since n is even and $\gcd(v, n) = 1$, $\gcd(v, 2n) = 1$. Hence, by Lemma 1.10.4, $\deg(\cos(2v\pi/2n)) = \phi(2n)/2$, Since n is even, $\phi(2n) = 2\phi(n)$ so $\deg(\cos(v\pi/n)) = \phi(n)$. ▮

1.3 deg (sin ($v\pi/n$)) Via Field Theory

Lemma 1.12 *If* $n = 4m$ *then* $[\mathsf{Q}(\zeta_{4m}) : \mathsf{Q}(\zeta_m)] = 2$.

Proof:

$\zeta_{4m} = e^{\pi i/2m}$
$\zeta_m = e^{2\pi i/m}$
$[\mathsf{Q}(\zeta_{4m}) : \mathsf{Q}(\zeta_m)]$
BILL: NEED TO PROVE THIS

▮

Lemma 1.13 *Let* $m \ge 5$ *be such that* $m \equiv 1 \pmod 4$ *(NOTE- WE MAY NOT NEED THIS). Then* $[\mathsf{Q}(\zeta_m) : \mathsf{Q}(\cos(\pi/m)] = 2$.

Proof:

By Lemma 1.10.2 $[\mathsf{Q}(\zeta_m) : \mathsf{Q}(\cos(2\pi/m)] = 2$.

CAN WE USE THIS?

ACTUALLY LEMMA 1.10.2 SAYS THAT IF $\gcd(v, m) = 1$ THEN $[\mathsf{Q}(\zeta_m^v) : \mathsf{Q}(\cos(2\pi v/m)] = 2$. MIGHT THAT HELP? ▮

Theorem 1.14 *Let* $n \equiv 4 \pmod{16}$ *and* $n \geq 20$. *Then*

$$[\mathsf{Q}(\zeta_n) : \mathsf{Q}(\sin(2\pi/n))] = 4.$$

Proof: Let $n = 16k + 4 = 4(4k + 1)$. Let $m = 4k + 1$. Note that $m \equiv 1 \pmod 4$. Let $r = (m - 1)/4$. Then

$$\frac{2\pi}{n} + \frac{2\pi r}{m} = \frac{2\pi}{4m} + \frac{2\pi r}{m} = \frac{\pi}{2m} + \frac{4\pi r}{2m} = \frac{\pi}{2m} + \frac{(m-1)\pi}{2m} = \frac{\pi}{2}.$$

Hence $\sin(2\pi/n) = \cos(2\pi r/m)$. (We are using the high school fact that $\cos(\theta) = \sin(\pi/2 - \theta)$.) So

$$[\mathsf{Q}(\zeta_n) : \mathsf{Q}(\sin(2\pi/n)] = [\mathsf{Q}(\zeta_n) : \mathsf{Q}(\cos(2\pi r/m)].$$

So we need to find $[\mathsf{Q}(\zeta_n) : \mathsf{Q}(\cos(2\pi r/m)]$. We first look at the angle

$$\frac{2\pi r}{m} = \frac{2(m-1)\pi}{4m} = \frac{(m-1)\pi}{m} = \pi - \frac{\pi}{m}.$$

$$\cos\left(\frac{2\pi r}{m}\right) = \cos\left(\pi - \frac{\pi}{m}\right) = -\cos\left(\frac{\pi}{m}\right).$$

So

$$[\mathsf{Q}(\zeta_n) : \mathsf{Q}(\cos(2\pi r/m)] = [\mathsf{Q}(\zeta_n) : \mathsf{Q}(-\cos(\pi/m)] = [\mathsf{Q}(\zeta_n) : \mathsf{Q}(\cos(\pi/m)]$$

$$= [\mathsf{Q}(\zeta_n) : \mathsf{Q}(\zeta_m)][\mathsf{Q}(\zeta_m) : \mathsf{Q}(\cos(\pi/m))].$$

By Lemma 1.12, $[\mathsf{Q}(\zeta_n) : \mathsf{Q}(\zeta_m] = 2$. By Lemma 1.13, $[\mathsf{Q}(\zeta_m) : \mathsf{Q}(\cos(\pi/m)] = 2$. Hence we have

$$[\mathsf{Q}(\zeta_n) : \mathsf{Q}(\cos(2\pi r/m)] = [\mathsf{Q}(\zeta_n) : \mathsf{Q}(-\cos(\pi/m)] = [\mathsf{Q}(\zeta_n) : \mathsf{Q}(\cos(\pi/m)] = 2 \times 2 = 4.$$

▮

IGNORE WHATS BELOW- NOT SURE IF I NEED IT

Lemma 1.15 *Let* $1 \leq v \leq n - 1$ *be such that* $\gcd(v, n) = 1$. *Let* $\zeta_n = e^{2\pi i/n}$.

1. $[Q(\zeta_n) : Q] = \phi(n)$.

2. $[\mathsf{Q}(\sin(2v\pi/n, i)) : \mathsf{Q}(\sin(2v\pi/n))] = 2$.

Proof:
1) By Fact 1.5 $[Q(\zeta_n) : Q] = \deg(\zeta_n)$. By Fact 1.9, $\deg(\zeta_n) = \phi(n)$. Hence $[Q(\zeta_n) : Q] = \phi(n)$.

2) By Fact 1.5,

$$[\mathsf{Q}(\sin(2v\pi/n, i)) : \mathsf{Q}(\sin(2v\pi/n))] = \deg_{\mathsf{Q}(\sin(2v\pi/n))}(i)].$$

Since $i \notin \mathsf{Q}(\sin(2v\pi/n))$,

$$\deg_{\mathsf{Q}(\sin(2v\pi/n))}(i)] \ge 2.$$

Since i is a root of $x^2 + 1$,

$$\deg_{\mathsf{Q}(\sin(2v\pi/n))}(i)] \le 2.$$

Hence

$$\deg_{\mathsf{Q}(\sin(2v\pi/n))}(i)] = 2.$$

▮

Lemma 1.16 *Let* $1 \le v \le n-1$ *be such that* $n \equiv 0 \pmod 4$ *and* $\gcd(v, n) = 1$. *Let* $\zeta_n = e^{2\pi i/n}$.

1. If n *is a power of 2 then* $[\mathsf{Q}(\zeta_n) : \mathsf{Q}(\sin(2v\pi/n, i))] = 1$.

2. If n *is not a power of 2 then* $[\mathsf{Q}(\zeta_n) : \mathsf{Q}(\sin(2v\pi/n, i))] = 2$.

Proof:
1) BILL: NEED PROOF

2) BILL: NEED PROOF
▮

Lemma 1.17 *Let* $1 \le v \le n-1$ *be such that* $n \equiv 0 \pmod 4$ *and* $\gcd(v, n) = 1$. *Let* $\zeta_n = e^{2\pi i/n}$.

1. If n *is a power of 2 then* $\deg(\sin(2v\pi/n) = \phi(n)/2$.

2. If n *is not a power of 2 then* $\deg(\sin(2v\pi/n) = \phi(n)/4$.

Proof:
1)

$$[\mathsf{Q}(\zeta_n) : \mathsf{Q}] = [\mathsf{Q}(\zeta_n) : \mathsf{Q}(\sin(2v\pi/n, i))][\mathsf{Q}(\sin(2v\pi/n, i)) : \mathsf{Q}(2v\pi/n)][\mathsf{Q}(2v\pi/n) : \mathsf{Q}].$$

- By Lemma 1.15.1$[\mathsf{Q}(\zeta_n):\mathsf{Q}]=\phi(n)$.
- By Lemma 1.18.1 $[\mathsf{Q}(\zeta_n):\mathsf{Q}(\sin(2v\pi/n,i))]=1$.
- By Lemma 1.16.2 $[\mathsf{Q}(\sin(2v\pi/n,i)):\mathsf{Q}(2v\pi/n)][\mathsf{Q}(2v\pi/n):\mathsf{Q}]=2$.

Hence we have

$$\phi(n)=1\times 2\times[\mathsf{Q}(2v\pi/n):\mathsf{Q}]$$

So

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

2)
$[\mathsf{Q}(\zeta_n):\mathsf{Q}]=[\mathsf{Q}(\zeta_n):\mathsf{Q}(\sin(2v\pi/n,i))][\mathsf{Q}(\sin(2v\pi/n,i)):\mathsf{Q}(\sin(2v\pi/n))][\mathsf{Q}(\sin(2v\pi/n)):\mathsf{Q}]$.

- By Lemma 1.15.1$[\mathsf{Q}(\zeta_n):\mathsf{Q}]=\phi(n)$.
- By Lemma 1.18.2 $[\mathsf{Q}(\zeta_n):\mathsf{Q}(\sin(2v\pi/n,i))]=2$.
- By Lemma 1.16.2 $[\mathsf{Q}(\sin(2v\pi/n,i):\mathsf{Q}(\sin(2v\pi/n))][\mathsf{Q}(\sin(2v\pi/n)):\mathsf{Q}]=2$.

Hence we have

$$\phi(n)=2\times 2\times[\mathsf{Q}(\sin(2v\pi/n)):\mathsf{Q}]$$

So

$$[\mathsf{Q}(\sin(2v\pi/n)):\mathsf{Q}]=\frac{1}{4}\phi(n).$$

▮

Lemma 1.18 *Let* $0\le v\le n$ *such that* $\gcd(v,n)=1$.

1. *If* n *is even then*
   (a) *If* n *is a power of 2 then* $\deg(\sin(v\pi/n)=\phi(n)$.
   (b) *If* n *is not a power of 2 then* $\deg(\sin(v\pi/n)=\phi(n)/2$.
2. *If* n *is odd then BILL FILL IN.*

Proof:
1) Since $n \equiv 0 \pmod 4$, $2n \equiv 0 \pmod 4$. Since $\gcd(v,n) = 1$, v is odd, so $\gcd(n, 2n) = 1$. Note that

$$\sin(v\pi/n) = \sin(2v\pi/2n).$$

If n is a power of 2 then $2n$ is a power of 2 so, by Lemma 1.18.1,

$$\deg(\sin(v\pi/n)) = \frac{1}{2}\phi(2n).$$

a) Let $n = 2^k$. Then

$$\frac{1}{2}\phi(2n) = \frac{1}{2}\phi(2^{k+1}) = \frac{1}{2}2^k = 2^{k-1} = \phi(n).$$

If n is not a power of 2 then $2n$ is not a power of 2 so, by Lemma 1.18.2.

$$\deg(\sin(v\pi/n)) = \frac{1}{4}\phi(2n).$$

b) Let $n = 2^k m$ where m is odd. Then

$$\frac{1}{4}\phi(2n) = \frac{1}{4}\phi(2^{k+1}m) = \frac{1}{4}2^k\phi(m) = 2^{k-2}\phi(m)$$

$$= \frac{1}{2}2^{k-1}\phi(m) = \frac{1}{2}\phi(2^k)\phi(m) = \frac{1}{2}\phi(2^k m) = \frac{1}{2}\phi(n).$$

2) $\sin(v\pi/n) = \sin(2 \times 2v\pi/4n)$.

BILL: I don't see how to get this in the form $\sin(2v'\pi/n')$ where $n' \equiv 0 \pmod 4$ and $\gcd(v', n') = 1$. ∎