Q Notes

By Peter Montgomery

November 26, 2020

Contents

Chapter 1

Complex Arithmetic

1.1 Complex Dot Product

The dot product definition for real vectors states that

$$\vec{a} \cdot \vec{b} = \sum_i \alpha_i \beta_i = \alpha_T \beta;\ \alpha, \beta \in \mathbb{R}$$

Which naturally leads to

$$|\vec{a}| = \sqrt{\vec{a} \cdot \vec{a}} \geq 0, \in \mathbb{R}$$

Ex. $\vec{v} = \begin{pmatrix} 3 \\ 2 \end{pmatrix}, |\vec{v}|^2 = \vec{v} \cdot \vec{v} = \begin{pmatrix} 3 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix} = 9 + 4 = 13 \Rightarrow |\vec{v}| = \sqrt{13}$

However, for complex vectors, $\vec{a} \cdot \vec{a}$ could be negative and leads to $|\vec{a}| \in \mathbb{C}$.

So, using the above dot product definition, for $\vec{v} = \begin{pmatrix} 3i \\ -2 \end{pmatrix}$,

$|\vec{v}|^2 = \vec{v} \cdot \vec{v} = 9(i^2) + 4 = -9 + 4 = -5 \ \therefore\ |\vec{v}| = \sqrt{-5}$

However, the magnitude of a vector can't be a complex value!

Complex Conjugate

For $\vec{\gamma} = \begin{pmatrix} a + ib \\ c + id \end{pmatrix}, \vec{\gamma}* = \begin{pmatrix} a - ib \\ c - id \end{pmatrix}$

Conjugation is distributive across sums and products.

$$(\alpha + \beta)^* = \alpha^* + \beta^*$$

$$(\alpha \times \beta)^* = \alpha^* \times \beta^*$$

Complex Dot Product

Now, the dot product definition changes:

$$\vec{\alpha} \cdot \vec{\beta} = (\vec{\alpha}_T)^* \cdot \vec{\beta}$$

This implies

$$\vec{\alpha} \cdot \vec{\alpha} = \vec{\alpha_T^*}\vec{\alpha} \in \mathbb{R}^+$$

For the above problem,

$$|\vec{v}|^2 = \vec{v} \cdot \vec{v} = (\vec{v}_T)^* \vec{v} = \begin{pmatrix} -3i & -2 \end{pmatrix} \begin{pmatrix} 3i \\ -2 \end{pmatrix} = -9(i^2) + 4 = 13 \Rightarrow |\vec{v}| = \sqrt{13} \in \mathbb{R}^+$$

This definition gives non-negative real magnitude to all complex vectors because

$$(a + bi)(a - bi) = a^2 + b^2, \; \forall \, a, b \in \mathbb{R}$$

α_T^* is also called the Hermitian conjugate $\equiv \alpha^\dagger$ (alpha-dagger).

Exercise: Proof that all n-dimensional complex vectors have real magnitude from the complex dot product definition

1.2 Complex Polar Form

Any complex number can be transformed from the form $z = a + bi$ to the form $z = r(\cos\theta + i\sin\theta)$, where $r = \sqrt{a^2 + b^2}$ & $\theta = \tan^{-1}\left(\frac{b}{a}\right)$.

From Euler's formula, this becomes

$$z = re^{i\theta}$$

For example,

$$1 + i = \sqrt{2}\,(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}) = \sqrt{2}\,e^{i\frac{\pi}{4}}$$

Some Results of Euler's Formula

For $z = e^{i\theta}$ & $w = e^{i\phi}$,

Multiplication: $zw = rs\,e^{i\theta + \phi}$

Division: $\frac{z}{w} = \frac{r}{s}\,e^{i\theta - \phi}$

Conjugation: $z^* = re^{-i\theta}$

1.3 Roots of Unity

For $z \in \mathbb{R}$ & $n \in \mathbb{Z}$, there are two solutions to the equation $z^n = 1$ $(z = \pm 1)$

The number of solutions depends on the power n: 2 for even n, 1 for odd n.

However, when the domain of z is extended to complex numbers, there are n unique complex solutions for every n.

In the complex polar form,

$$z^n = e^{i\theta n} = 1$$

$$e^{i(n\theta)} = \cos(n\theta) + i\sin(n\theta) = 1 + 0i$$

We can solve either equations to get θ

$$\cos(n\theta) = 1 \text{ or } \sin(n\theta) = 0$$

Both leads to

$$\theta = \frac{2\pi k}{n}, k \in \mathbb{Z}_{\geq 0}$$

Notice that (**Excercise: Proof this**)

$$e^{i\frac{2\pi k}{n}} = e^{i\frac{2\pi(k+an)}{n}}$$

We can define arbitrary set $\mathcal{R}_n$ to be the set of all k, where

$$f(k) \equiv e^{i\frac{2\pi}{n}k} \text{ is unique}$$

From above, we can deduce a periodicity in the range of this function, where

$$f(\mathcal{R}_n) = f(\mathcal{R}_n + an)$$

In fact, $\mathcal{R}_n$ is a least residue system modulo n. This just means that we can use the properties of modular arithmetic on $\mathcal{R}_n$.

$$f(\mathcal{R}_n) = f(\mathcal{R}_n \bmod n)$$

Going back the roots of unity,

$$z = e^{i\frac{2\pi}{n}(k \bmod n)},\ k \bmod n \in \{0, ..., n-1\}$$

Thus,

$$z^n = 1$$

In some context, z is written as ω_n, so in summary

$$(\omega_n)^k = \sqrt[n]{1} = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right) = e^{i\frac{2\pi}{n}k},\ k \in \{0, ..., n-1\}$$

For example, $\sqrt[5]{1} = 0.309 + 0.951i\ \&\ -0.809 - 0.5878i\ \&\ 3$ other numbers

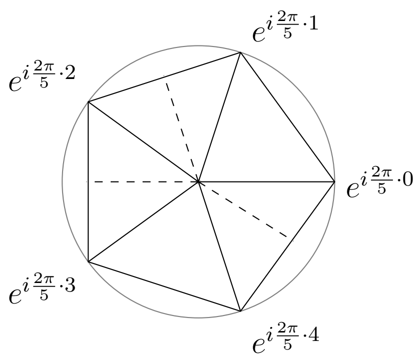
1.4 Summing Roots of Unity

The sum of all root nth root of unity is 0

$$\sum_{k=0}^{n-1}(\omega_n)^k = 0$$

Geometric Proof

- To prove this geometrically, draw all the $(\omega_n)^k$ as vectors with origin at 0 in the complex plane.
- Connect the end of the vectors together to end up with an n-sided regular.
- Notice that each vector is perpendicular to the opposite side of the polygon, so each can be seen as a scaled up and rotated version the polygon side.
- Because the differences of the angle between two adjacent vectors is $\frac{2\pi}{n}$ (same as the polygon), when put end to end, the vectors will form a close loop that is another n-sided regular polygon.
- This means that the sum of the vector ends up at the origin and thus is 0



An n = 5 example from SunilK

Algebraic Proof

Let

$$\sum_{k=0}^{n-1}(\omega_n)^k = A$$

Going back to set $\mathcal{R}_n$ from above above, define a function S for which

$$S(\mathcal{R}_n) = \sum_{k=0}^{n-1} \omega^k \;\; (\omega \equiv \omega_n)$$

To repeat, $\mathcal{R}_n$ is a cyclic group of order n with integer and modular addition. In other words, $\mathcal{R}_n$ is the set integers modulo n). A property of $\mathcal{R}_n$ is

$$\mathcal{R}_n = \mathcal{R}_n + \alpha \text{ (mod n)}, \; \alpha \in \mathbb{Z}$$

For example, let $\mathcal{R}_n = \{0, 1, 2, 3\}$, and $\alpha = 2$

$$\mathcal{R}_n + \alpha = \{2, 3, 4, 5\} \text{ (mod 4)} = \{0, 1, 2, 3\}$$

This implies that

$$S(\mathcal{R}_n) = (\mathcal{R}_n + \alpha)$$

Thus

$$\sum_{k=0}^{n-1} \omega^k = \sum_{k=0}^{n-1} \omega^{k+\alpha} = \omega^\alpha \sum_{k=0}^{n-1} \omega^k$$

Substituting from above

$$\omega^\alpha \times A = A$$

The trivial solution is $\omega^\alpha = 1$. However, we're trying to solve A

$$(\omega^\alpha - 1)A = 0 \;\therefore\; A = 0$$

In conclusion this result agrees with the geometric proof,

$$\sum_{k=0}^{n-1} \omega^k = 0$$

A More General Sum

A broader definition for the function S from above is S_a,

$$S_a(\mathcal{R}_n) = S(a \cdot \mathcal{R}_n \text{ (mod } n\text{) }) = \sum_{k=0}^{n-1} (\omega^k)^a, \; a \in \mathbb{Z}_{\geq 0, <n}$$

This is when every element in the $\mathcal{R}_n$ is mod-n multiplied by a constant a. The sum of roots of unity above, $S(\mathcal{R}_n)$, is the special case where $a = 1$.

Right off the bat, for the case $a = 0$, the sum evaluate to n, regardless of what n is.

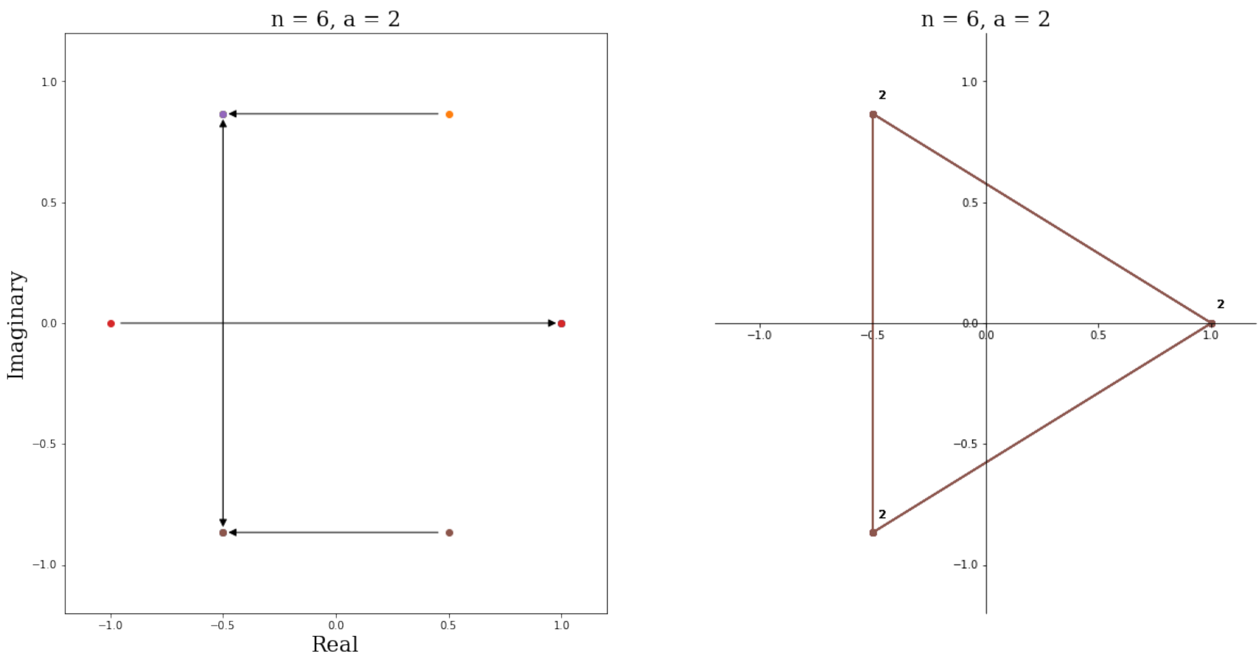
Evaluating the sum for $a > 1$ requires making some assumptions.

Conjecture 1

The operation $a \cdot \mathcal{R}_n \pmod{n}$ collapses the cyclic group $\mathcal{R}_n$ uniformly into a smaller cyclic group that is a factor of n.

$$a \cdot \mathcal{R}_n \pmod{n} \longrightarrow \mathcal{R}_\phi,\ \phi = \frac{n}{\gcd(n, a)}$$

The digram shows the geometric representation of the $n = 6, a = 2$ example, where the hexagon is collapsed into a triangle.



An n = 6, a = 2 example

The left figure shows the mapping of points by S_a.

$$2 \cdot \{0, 1, 2, 3, 4, 5, 6\} \pmod{n} = \{0, 2, 4, 0, 2, 4\} = 2 \text{ sets of } \{0, 2, 4\}$$

The right figure shows the end-result of the mapping. The number on top of the vertex is the number of points mapped into that coordinate.

Running a Monte Carlo simulation of $100,000$ shots on this conjecture on Python 3.6 & 3.7 confirms this result 100% for $n < 100,000$.

Assuming Conjecture 1 is true, this implies that

$$a \cdot \mathcal{R}_n \pmod{n} \to \left(\tfrac{n}{\phi}\right) \text{ identical sets of } \mathcal{R}_\phi$$

This means that

$$S_a(\mathcal{R}_n) = S(a \cdot \mathcal{R}_n \pmod{n}\,) = S\left(\tfrac{n}{\phi} \cdot \mathcal{R}_\phi\right)$$

Because S_a is a sum (linear operator), we can bring the $\frac{n}{\phi}$ outside of the sum.

$$S\left(\tfrac{n}{\phi}\cdot\mathcal{R}_\phi\right)=\frac{n}{\phi}\cdot S\left(\mathcal{R}_\phi\right)=\frac{n}{\phi}\cdot\sum_{k=0}^{\phi-1}\omega^k$$

We have already prove that the sum of roots of unity equals 0. This means that our sum also equals 0. In summary,

$$S_a(\mathcal{R}_n)=\sum_{k=0}^{n-1}(\omega^k)^a=\begin{cases}n, & a=0\\ 0, & 0<a<n\end{cases}$$

1.5 Kronecker Delta

The Kronecker delta is a useful notation to expresses a result to be 0 for all index, except index m, where the the result is 1.

$$\delta_{jm}=\begin{cases}1, & \text{if } j=m\\ 0, & \text{otherwise}\end{cases}$$

Expressing the general sum above using the Kronecker delta,

$$\sum_{k=0}^{n-1}(\omega^k)^a=\sum_{k=0}^{n-1}\omega^{(j-m)k}=n\cdot\delta_{jm}$$