Number of Elements in the Group Generated by A and B

Saad Khalid

December 1st, 2015

Proving the group generated by A^j has n elements

$$A = \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}$$

Lemma

Before our main proof, we will propose that:

$$A^j = \begin{bmatrix} \cos\frac{2j\pi}{n} & -\sin\frac{2j\pi}{n} \\ \sin\frac{2j\pi}{n} & \cos\frac{2j\pi}{n} \end{bmatrix}$$

for $j \in \mathbb{Z}^+$

Proof

We begin by noticing that:

$$A^2 = \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix} \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}$$
$$= \begin{bmatrix} \cos^2(\frac{2\pi}{n}) - \sin^2(\frac{2\pi}{n}) & -2\cos(\frac{2\pi}{n})\sin(\frac{2\pi}{n}) \\ -2\cos(\frac{2\pi}{n})\sin(\frac{2\pi}{n}) & \cos^2(\frac{2\pi}{n}) - \sin^2(\frac{2\pi}{n}) \end{bmatrix}$$

Using the Double Angle Formulas, we know:

$$\cos 2u = \cos^2 u - \sin^2 u$$

$$\sin 2u = 2 \sin u \cos u$$

So,

$$\begin{bmatrix} \cos^2(\frac{2\pi}{n}) - \sin^2(\frac{2\pi}{n}) & -2\cos(\frac{2\pi}{n})\sin(\frac{2\pi}{n}) \\ \\ 2\cos(\frac{2\pi}{n})\sin(\frac{2\pi}{n}) & \cos^2(\frac{2\pi}{n}) - \sin^2(\frac{2\pi}{n}) \end{bmatrix} = \begin{bmatrix} \cos\frac{4\pi}{n} & -\sin\frac{4\pi}{n} \\ \\ \sin\frac{4\pi}{n} & \cos\frac{4\pi}{n} \end{bmatrix}$$

Now, let's assume this formula is true for $j = 1, 2, 3, ..., x - 1$
Then,

$$A^j = AA^{j-1} = \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix} \begin{bmatrix} \cos\frac{2(j-1)\pi}{n} & -\sin\frac{2(j-1)\pi}{n} \\ \\ \sin\frac{2(j-1)\pi}{n} & \cos\frac{2(j-1)\pi}{n} \end{bmatrix}$$

Using the Sum-Difference Formulas for Trigonometric Functions:

$$= \begin{bmatrix} \cos(\frac{2\pi+2\pi j-2\pi}{n} & -\sin(\frac{2\pi+2j\pi-2\pi}{n} \\ \\ \sin(\frac{2\pi+2j\pi-2\pi}{n} & \cos(\frac{2\pi+2\pi j-2\pi}{n} \end{bmatrix}$$

Now using the Double Angle Formulas:

$$= \begin{bmatrix} \cos\frac{2j\pi}{n} & -\sin\frac{2j\pi}{n} \\ \\ \sin\frac{2j\pi}{n} & \cos\frac{2j\pi}{n} \end{bmatrix}$$

Hence, we conclude our proof.

Since, for $j \in \mathbb{Z}^+$,

$$A^j = \begin{bmatrix} \cos\frac{2j\pi}{n} & -\sin\frac{2j\pi}{n} \\ \\ \sin\frac{2j\pi}{n} & \cos\frac{2j\pi}{n} \end{bmatrix}$$

It is obvious that when $j = n$, A^j decomposes to:

$$\begin{bmatrix} \cos 2\pi & -\sin 2\pi \\ \sin 2\pi & \cos 2\pi \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I = A^0$$

So, $A^j = I$ when $|j| = n$.

Lemma: $A^j = A^{j+n}$

$$A^{j+n} = A^j A^n = A^j I = A^j$$

We now know that $A^j = A^{j+n}$. That is to say, A^j repeats for every n increase in its exponent.
Hence, the group generated by A^j has unique elements for $j = (1+kn, 2+kn, 3+kn, .., n+kn)$ where $k \in \mathbb{Z}$. Hence, it has n unique elements.

Proving the group generated by B has 2 elements

$$B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$B^2 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

We can now write now write B^3 as $BB^2 = BI = B$.
This pattern continues, and this $B^k = B$ for all k that are odd, and $B^k = I$ for all k that are even.
Hence, the group generated by B has 2 elements.

Proving $A^j B = BA^{-j}$

We can see that this relationship is true for $j = 1$
First, we note that:

$$A^{-1} = \begin{bmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ & \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix}$$

Then,

$$BA^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ & \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix} = \begin{bmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & -\cos\frac{2\pi}{n} \end{bmatrix}$$

$$= \begin{bmatrix} \cos\frac{2\pi}{n} & -\sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = AB$$

Then, we can see that

$$BA^{-2} = BA^{-1}A^{-1} = ABA^{-1} = AAB = A^2B$$

Assume this is true for $j = 1, 2, 3, 4, ..., x - 1$

Then, for $j = x$, we see that:

$$A^xB = AA^{x-1}B = ABA^{1-x} = BA^{-1}A^{1-x} = BA^{-x}$$

Hence, we have proven the relationship by PCI.

Conclusion

Hence, we can show that the group generated by A and B has 2n elements.
The group has all unique A^jB^k and B^kA^j.
However, we have proven that $B^kA^j = A^{-j}B^k$, so we can instead consider all unique A^jB^k and $A^{-j}B^k$.
We have also proven that any A^j can be written as A^{j+n}. So, any A^j with a negative value for j can be written instead with a positive exponent.
So, we are only concerned with A^jB^k. We know that A^j has n possible values, as we saw in our earlier proof(it is unique for $j = 1, 2, 3, 4, ..., n$).
We also have proven that B^k has two possible values. Therefore, the group generated by A and B have $2n$ possible values.