The Number Of Generators Of A Cyclic Group

Edward McAndrew, Evan O'Brien and Padraig O'Shea
MA3343 Groups

NUI Galway
OÉ Gaillimh

What is a cyclic group?

A cyclic group is a group that is generated by a single element. It is a set of invertible elements with a single associative binary operation. It also contains an element X(called the group generator) such that all of the other elements contained in the group can be obtained by applying the group operation to the element X or its inverse. All cyclic groups are abelian.

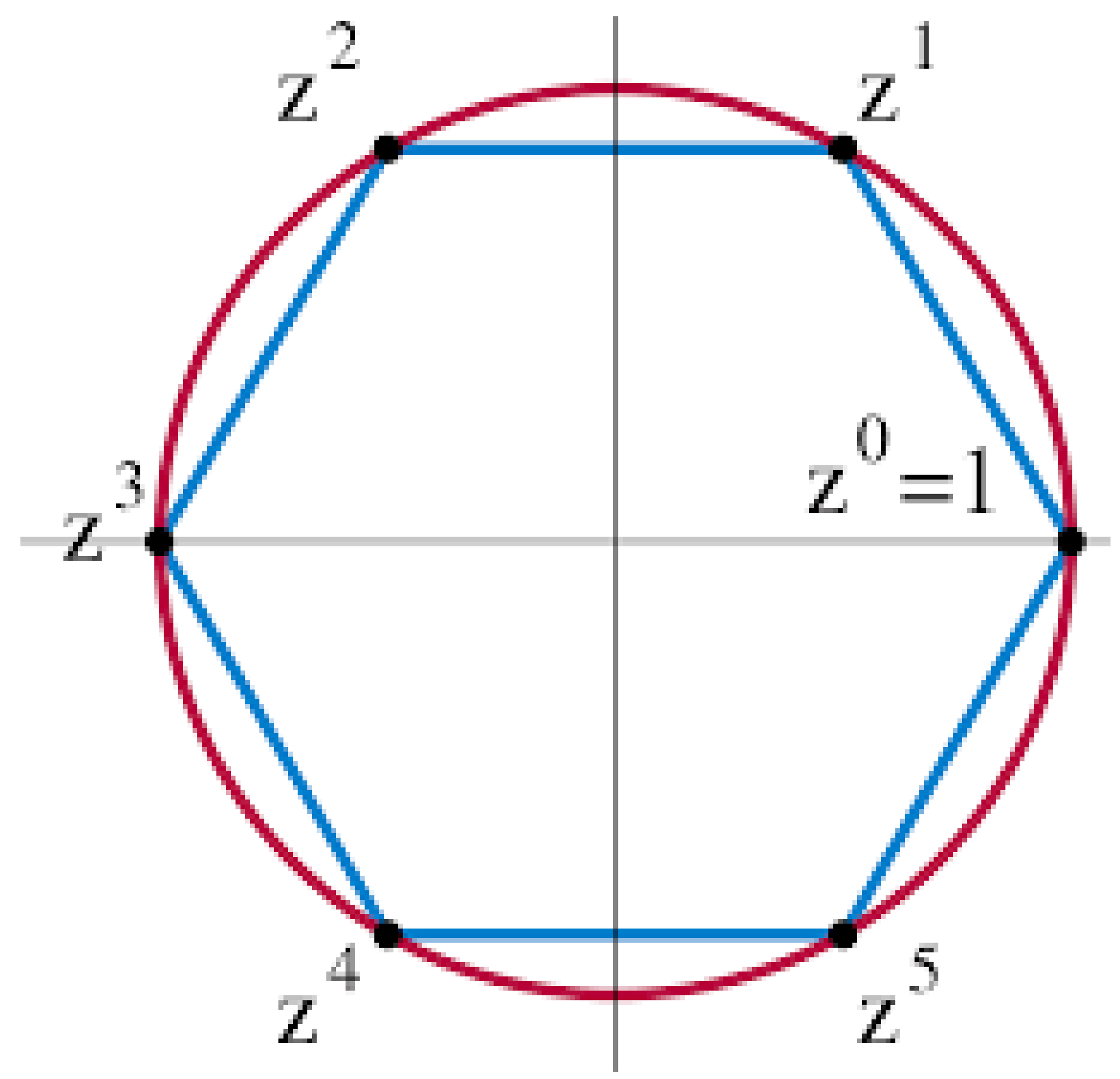
How many different elements of a cyclic group of order n are generators of the group?

If your cyclic group has order n, there will be one generator for every number between 1 and n1 (inclusive) that is relatively prime to n: in other words, there are phi(n) generators, where phi is Euler's totient function.

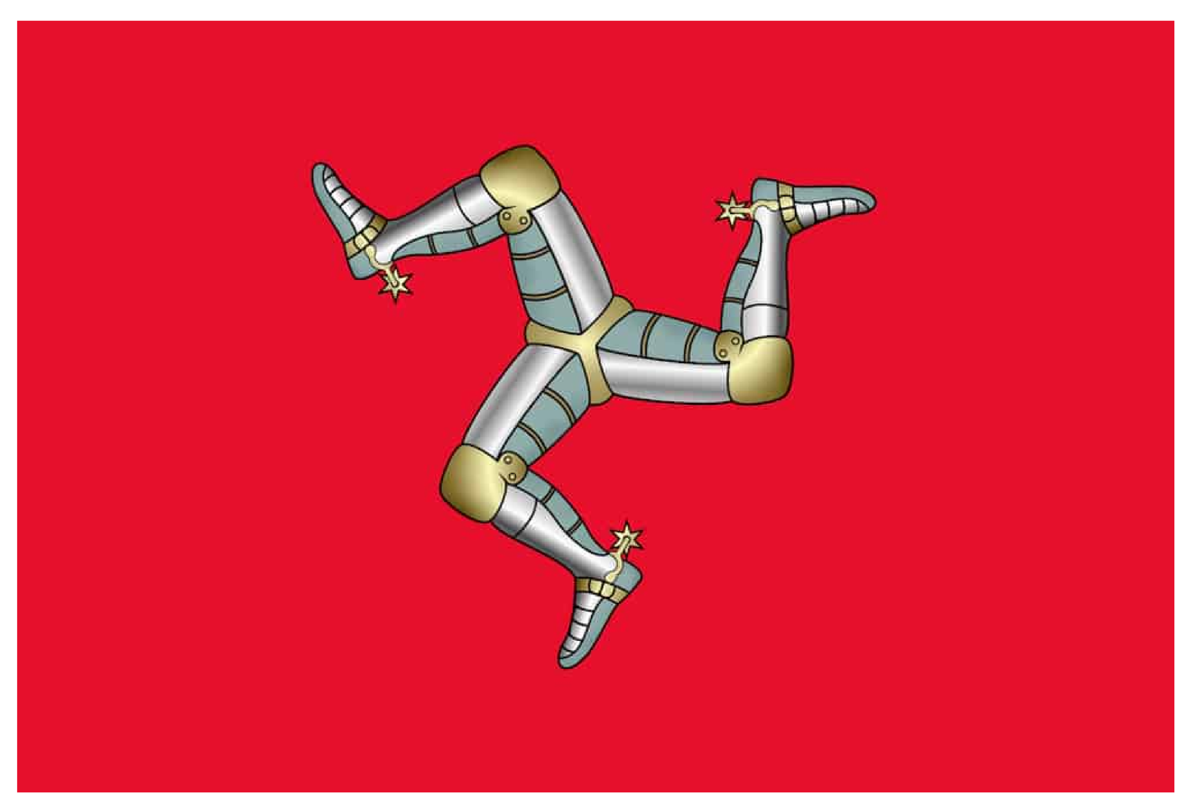
What does the answer have to do with the number n?

The amount of generators a cyclic group are relatively prime to the order of group.
For Example: 8(Which is Z8=(0,1,2,3,4,5,6,7)
<0> = (0)
<1> = (1,2,3,4,5,6,7,0)= (0,1,2,3,4,5,6,7)=Z8
<2> = (2,4,6,0)= (2,4,6,0)
<3> = (3,6,1,4,7,2,5,0)= (0,1,2,3,4,5,6,7)=Z8
<4> = (0,4)
<5> = Z8
<6> = (0,2,4,6)
<7> = Z8
Notice a Pattern? If it's relatively prime to 8, it generates Z8. This proves that all the generators in a cyclic group are relatively prime to the order of the group..

Cyclic Group



The six 6th complex roots of unity form a cyclic group under multiplication. Here z is generator, but z2 is not, because its powers fail to produce the odd powers of z.



The Isle of Man flag is an example of a cyclic group in rotational symmetry

What are generators in group theory?

A set of generators (g1,...,gn) is a set of group elements such that possibly repeated application of the generators on themselves and each other is capable of producing all the elements in the group. Cyclic groups can be generated as powers of a single generator. Two elements of a dihedral group that do not have the same sign of ordering are generators for the entire group.

How many generators does an infinite cyclic group have?

An infinite cyclic group can only have 2 generators.
Proof:
If G = <a> then G also equals <a^{-}1 >,
because every element a$^{n}of < a >$
is also equal to (a^{-}1)$^{-}n.$
If G = <a> = <b> then b = a^{n}
for some n and a = b^{m}
for some m.
Therefore = b^{m} = $(a^{n})^{m} = a^{n}m$
Since G is an infinite cyclic group nm must equal to 1 , nm = 1 has only two solutions (1,1) and (-1,-1) .
These give b = a or b = a^{-}1
Therefore an infinite cyclic group can only have two generators .