The Number of Generators of a Cyclic Group

Sarah Skeffington & Griffen Small

School of Mathematics, Statistics & Applied Mathematics, National University of Ireland, Galway

1 Introduction

This poster is concerned with cyclic groups. In particular, we are interested in counting the number of elements that generate such groups and how this number depends on the order of the group. We begin with a review of cyclic groups and generators, providing examples of each. Following this, we derive an interesting formula for the number of generators of a finite cyclic group. We finish with a similar result for infinite cyclic groups.

2 Cyclic Groups and Generators

Let G be a group and let $\langle x \rangle$ be the cyclic subgroup of G generated by $x \in G$. We say that G is **cyclic** if $G = \langle x \rangle$. Equivalently, a cyclic group G is one which can be built from a single element $x \in G$ by "taking powers". Any such element x is called a **generator** for G. Every cyclic group is necessarily abelian; see [1]. We illustrate these ideas with two well-known examples.

- Let G be the group of complex 6^{th} roots of unity under multiplication

$$G = \left\{1, e^{\frac{\mathrm{i}\pi}{3}}, e^{\frac{2\mathrm{i}\pi}{3}}, e^{\mathrm{i}\pi}, e^{\frac{4\mathrm{i}\pi}{3}}, e^{\frac{5\mathrm{i}\pi}{3}}\right\}.$$

  The group is cyclic since it is generated by (for example) $x = e^{\mathrm{i}\pi/3}$; that is,

$$G = \langle x \rangle = \left\{\mathrm{id}, x, x^2, x^3, x^4, x^5\right\}, \tag{1}$$

  where $\mathrm{id} = 1$ and $x^6 = 1$. This is not the only generator for G: it is also generated by $x = e^{5\mathrm{i}\pi/3}$. It turns out that $x = e^{\mathrm{i}\pi/3}$ and $x = e^{5\mathrm{i}\pi/3}$ are the only two generators for G; see Figure 1.

- Let $G = (\mathbb{Z}, +)$ be the group of integers under addition. The group is cyclic since it is generated by (for example) $x = 1$; that is,

$$G = \langle x \rangle = \left\{\ldots, x^{-2}, x^{-1}, \mathrm{id}, x, x^2, \ldots\right\}, \tag{2}$$

  where $\mathrm{id} = 0$ and $x^n = n$. As before, this is not the only generator: $x = -1$ also generates G. It turns out that $x = 1$ and $x = -1$ are the only two generators for G.

These examples, specifically (1) and (2), demonstrate that despite superficial differences, all cyclic groups have the same abstract form. To be more precise, all cyclic groups of the same order are **isomorphic** to each other [2]. Hence we adopt a single notation $C_n = \langle x \rangle$ for all cyclic groups of order n; here it is understood that $x^n = \mathrm{id}$.

We now turn to the problem of counting the number of generators x for a given order n. First, we consider the finite case.

3 The Finite cyclic group C_n

Theorem 3.1. *Suppose that x is a generator of the finite cyclic group C_n. Then the elements of C_n that generate it as a cyclic group are exactly those elements of the form x^k, where $\gcd(k, n) = 1$. The number of these is $\phi(n)$: the Euler totient function.*

The main idea of the proof of Theorem 3.1 is to show that $C_n = \langle x^k \rangle$ if and only if $\gcd(k, n) = 1$; we say that the integers k and n are **coprime** if $\gcd(k, n) = 1$. Before giving a proof we state without proof the following result from [3]:

Lemma 3.2. *Two integers a and b are coprime if and only if there exists integers s and t such that $sa + tb = 1$.*

Proof. First, we show that $C_n = \langle x^k \rangle$ if k and n are coprime (the **sufficient condition**). By Lemma 3.2, there exists integers u and v such that $uk + vn = 1$. Then, for integral m, we have

$$\begin{aligned} x^m &= x^{m(uk+vn)} \\ &= x^{muk} x^{mvn} \\ &= (x^k)^{mu} (x^n)^{mv} \\ &= (x^k)^{mu}, \end{aligned}$$

since $x^n = \mathrm{id}$. Since the elements of C_n are exactly those of the form x^m, it follows that every element of C_n is a power of x^k, and therefore $C_n = \langle x^k \rangle$. Thus, $C_n = \langle x^k \rangle$ if k and n are coprime.

Second, we show that if $C_n = \langle x^k \rangle$, then k and n are coprime (the **necessary condition**). Since x^k generates C_n, there exists an integer u such that

$$x = (x^k)^u = x^{uk}. \tag{3}$$

Multiplying both sides of (3) by x^{-1}, we have

$$x^{uk-1} = \mathrm{id}. \tag{4}$$

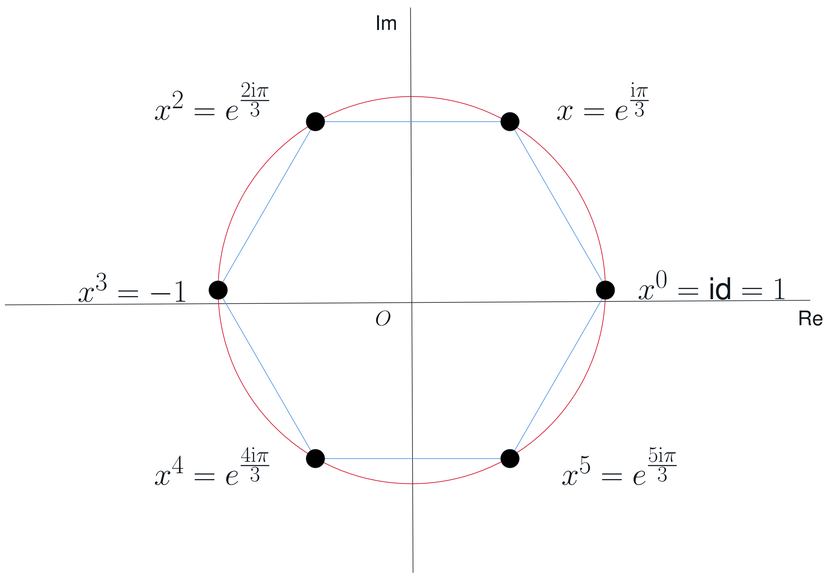

Fig. 1: The complex 6^{th} roots of unity form a cyclic group under multiplication. It is easily seen that $x = e^{\mathrm{i}\pi/3}$ and $x = e^{5\mathrm{i}\pi/3}$ are the only two generators for G .

For (4) to hold we must have that n divides $uk - 1$ (since $x^n = \mathrm{id}$). Hence there exists an integer $-v$ such that $uk - 1 = -vn$ or, equivalently, $uk + vn = 1$. It follows from Lemma 3.2 that k and n are coprime. Thus, k and n are coprime if $C_n = \langle x^k \rangle$.

We conclude that $C_n = \langle x^k \rangle$ if and only if k and n are coprime, i.e., $\gcd(k, n) = 1$. This means that $\gcd(k, n) = 1$ is a necessary and sufficient condition for x^k to generate C_n. Hence the number of distinct elements of C_n that generate it as a cyclic group is equal to the number of positive integers $k \leq n$ for which $\gcd(k, n) = 1$. The number of these is $\phi(n)$. ■

As an example, the number of distinct elements of C_6 (which we can think of as the group of complex 6^{th} roots of unity under multiplication) that generate it as a cyclic group is $\phi(6) = 2$, as claimed in § 2.

Next, we consider the infinite case.

4 The Infinite Cyclic Group C_∞

Theorem 4.1. *Suppose that x is a generator of the infinite cyclic group C_∞. Then the elements of C_∞ that generate it as a cyclic group are x and x^{-1}. So C_∞ has exactly two generators.*

Proof. First, we show that if $C_\infty = \langle x \rangle$, then $C_\infty = \langle x^{-1} \rangle$. For integral m, we have $(x^{-1})^m = x^{-m}$. Since the elements of C_∞ are exactly those of the form x^{-m}, it follows that every element of C_∞ is a power of x^{-1}, and therefore $C_\infty = \langle x^{-1} \rangle$.

Second, we show that x and x^{-1} are the only two generators for C_∞. Since $C_\infty = \langle x \rangle = \langle x^{-1} \rangle$, we must have $x = (x^{-1})^a$ for some integer a and $x^{-1} = x^b$ for some integer b. These equations imply that $x = (x^{-1})^a = x^{ab}$. Since C_∞ is infinite cyclic, $ab = 1$, and so (a, b) is either $(1, 1)$ or $(-1, -1)$. Thus, the only generators of C_∞ are x and x^{-1}. ■

We note that Theorem 4.1 is consistent with our example in § 2 of the group $(\mathbb{Z}, +)$, which had exactly two generators: $x = 1$ and $x^{-1} = -1$.

5 Remark

Theorems 3.1 and 4.1 not only yield information about the number of generators but also their form. For example, Theorem 3.1 says that the $\phi(n)$ generators for the group of complex n^{th} roots of unity under multiplication all have the from $e^{2\mathrm{i}\pi k/n}$, where $\gcd(k, n) = 1$.

6 Summary

We have shown that the finite cyclic group C_n has exactly $\phi(n)$ generators and that the infinite cyclic group C_∞ has exactly two generators. We have also illustrated these results for the case of two well-known examples of cyclic groups: the group of complex n^{th} roots of unity under multiplication and the group $(\mathbb{Z}, +)$.

7 References

[1] C. Jordan & D. Jordan. *Groups*. Newnes, 2004, p. 58.

[2] J. Rotman. *Advanced Modern Algebra*. Prentice Hall, 2003, p. 75.

[3] P. Cohn. *Algebra Volume 1*. John Wiley & Sons, 1982, pp. 27–28.