Abstract Algebra I

Ji, Yong-hyeon

April 1, 2025

We cover the following topics in this note.

- Cyclic Group
- TBA

Note. Let $(G, *)$ be a group with identity element e. Recall that the axioms of a group require:

(G0) $\forall x, y \in G, x * y \in G$;

(G1) $\forall x, y, z \in G,\ (x * y) * z = x * (y * z)$;

(G2) $\exists e \in G,$ s.t. $\forall x \in G,\ e \cdot x = x \cdot e = x$;

(G3) $\forall x \in G,\ \exists x^{-1} \in G$ s.t. $x \cdot x^{-1} = x^{-1} \cdot x = e$.

Consider $(\mathbb{Z}, +)$ as the additive group of integers. For $a \in G$ and $n \in \mathbb{Z}$, the notation

$$a^n := \begin{cases} \underbrace{a * a * \cdots * a}_{n \text{ times}} & : n > 0, \\ e & : n = 0, \\ (a^{-1})^{-n} & : n < 0, \end{cases}$$

defines the n-th power of a.

Cyclic Group

Definition. A group G is said to be **cyclic** if and only if

$$\exists a \in G \text{ such that } \left[\forall g \in G,\ \exists n \in \mathbb{Z} \text{ with } g = a^n\right].$$

The element a is called a **generator** of G.

The Classification for Cyclic Groups

Theorem. *Let G be a cyclic group. Then*

$$G \simeq \begin{cases} \mathbb{Z} & \textit{if G is infinite,} \\ \mathbb{Z}/n\mathbb{Z} & \textit{if G is finite of order } n. \end{cases}$$

In other words, Every cyclic group G is isomorphic to either $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$.

Proof. Let G be a cyclic group and let $a \in G$ be a generator. Define the mapping

$$\varphi : (\mathbb{Z}, +) \longrightarrow (G, *), \quad \varphi(n) = a^n.$$

We now verify several properties of φ. □

Definition. G is called *cyclic* $\iff$ $\exists\, a \in G$ such that $G = \langle a \rangle := \{\, a^n \mid n \in \mathbb{Z} \,\}$.

In symbolic logic, this may be written as:

$$\exists\, a \in G \;\; \forall\, g \in G,\; \exists\, n \in \mathbb{Z} \text{ such that } g = a^n.$$

Here, the element a is called a *generator* of G. The notation a^n is understood in the group-theoretic sense, where for $n \geq 0$,

$$a^n = \underbrace{a \cdot a \cdots a}_{n \text{ factors}},$$

and for $n < 0$,

$$a^n = (a^{-1})^{-n}.$$

The structure of cyclic groups is completely determined by the order of any generator. Let $a \in G$ be a generator of the cyclic group G. Consider the homomorphism

$$\varphi : (\mathbb{Z}, +) \to (G, \cdot) \quad \text{defined by} \quad \varphi(n) = a^n.$$

Since G is cyclic, φ is surjective. The kernel of φ is given by

$$\ker(\varphi) = \{\, n \in \mathbb{Z} \mid a^n = e \,\},$$

where e denotes the identity element in G.

We now distinguish two cases:

1. **Infinite Case:** If no nonzero $n \in \mathbb{Z}$ satisfies $a^n = e$, then

$$\ker(\varphi) = \{0\}.$$

By the First Isomorphism Theorem,

$$G \cong \mathbb{Z}.$$

2. **Finite Case:** If there exists a least positive integer n_0 such that

$$a^{n_0} = e,$$

then

$$\ker(\varphi) = n_0\mathbb{Z} := \{\, n_0 k \mid k \in \mathbb{Z} \,\}.$$

Again by the First Isomorphism Theorem,

$$G \cong \mathbb{Z}/n_0\mathbb{Z}.$$

In this context, we say that G is of *finite order* n_0.

Thus, we have the following classification theorem:

$$\boxed{\text{Every cyclic group } G \text{ is isomorphic to either } \mathbb{Z} \text{ (if } |G| = \infty) \text{ or } \mathbb{Z}/n\mathbb{Z} \text{ for some } n \in \mathbb{N} \text{ (if } |G| = n < \infty).}$$

—

- **Existence of Generator:** $\exists\, a \in G$ such that $\forall\, g \in G, \exists\, n \in \mathbb{Z}$ with $g = a^n$.

- **Homomorphism Construction:** Define $\varphi : \mathbb{Z} \to G$ by $\varphi(n) = a^n$. This map is a group homomorphism with image G.

- **Kernel Analysis:** - If $\ker(\varphi) = \{0\}$, then $G \cong \mathbb{Z}$. - If $\ker(\varphi) = n\mathbb{Z}$ for some $n > 0$, then $G \cong \mathbb{Z}/n\mathbb{Z}$.

This completes the formal definition and classification of cyclic groups in an extremely rigorous and symbolic manner suitable for graduate-level presentation.

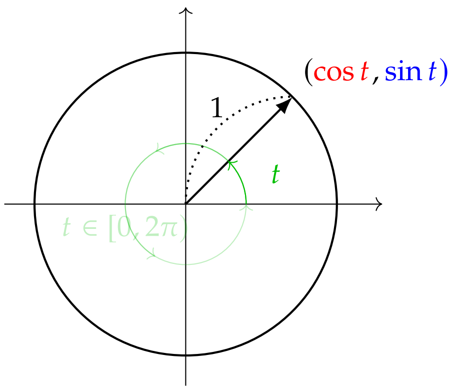
Proposition. *The subgroup of cyclic group is also cyclic.*

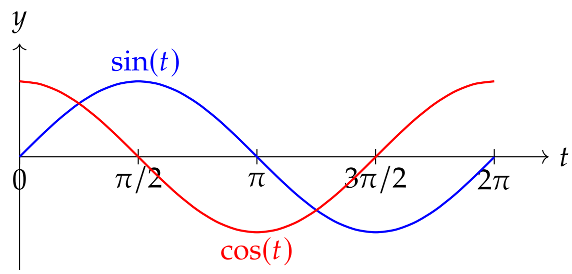
References

[1] 수학의 즐거움, Enjoying Math. "수학 공부, 기초부터 대학원 수학까지, 20. 추상대수학 (a) 순환군의 분류 Classification of cyclic group" YouTube Video, 22:01. Published October 18, 2019. URL: `https://www.youtube.com/watch?v=1yQ52OSB_Cc&t=708s`.

A Unit Circle

The set $\mathbb{S}^1 := \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ is called the **unit circle**.





The standard parametrization of $\mathbb{S}^1$ is given by

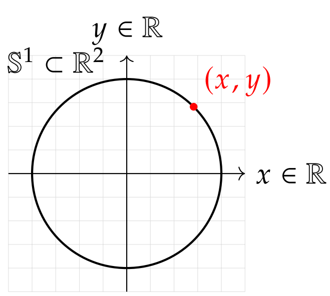
$$t \mapsto (\cos t, \sin t), \quad t \in [0, 2\pi),$$

which in turn implies the fundamental trigonometric identity $\cos^2 t + \sin^2 t = 1$. The mapping

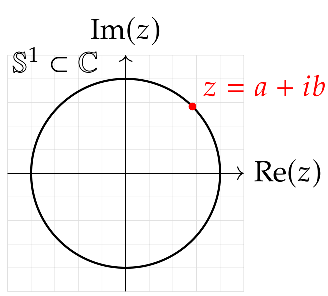
$$\begin{array}{rcccl} \varphi & : & [0, 2\pi) & \longrightarrow & \mathbb{S}^1 \\ & & t & \longmapsto & (\cos t, \sin t) \end{array}.$$

provides a bijection between the half-open interval $[0, 2\pi)$ and the unit circle $\mathbb{S}^1$.

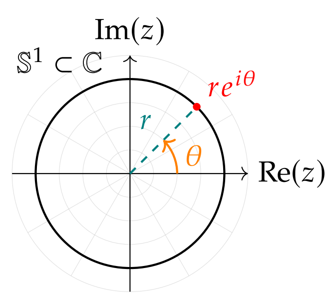
Geometrically, it represents the set of points at a fixed distance 1 from the origin in $\mathbb{R}^2$, while algebraically it can be seen as a group under complex multiplication.



$x^2 + y^2 = 1$



$|z| = 1$



$|r| = 1$ and $\theta \in \mathbb{R}$

The unit circle can be described in several equivalent ways. In $\mathbb{R}^2$, it is given by:

$$\mathbb{S}^1 = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}.$$

In the complex plane, we write:

$$\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\} = \{re^{i\theta} : |r| = 1 \text{ and } \theta \in \mathbb{R}\}.$$

We now show that S^1 forms a group under complex multiplication:

(G0) **(Closure)** Let $z_1 = e^{i\theta_1}$ and $z_2 = e^{i\theta_2} \in \mathbb{S}^1$. Then $z_1 z_2 = e^{i\theta_1} e^{i\theta_2} = e^{i(\theta_1+\theta_2)} \in \mathbb{S}^1$.

(G1) **(Associativity)** Let $z_1 = e^{i\theta_1}, z_2 = e^{i\theta_2}, z_3 = e^{i\theta_3} \in \mathbb{S}^1$ then

$$(z_1 z_2) z_3 = (e^{i\theta_1} e^{i\theta_2}) e^{i\theta_3} = e^{i(\theta_1+\theta_2)} e^{i\theta_3} = e^{i(\theta_1+\theta_2+\theta_3)} = e^{i\theta_1} e^{i(\theta_2+\theta_3)} = e^{i\theta_1}(e^{i\theta_2} e^{i\theta_3}) = z_1(z_2 z_3).$$

(G2) **(Identity Element)** For each $z = e^{i\theta} \in S^1$,

$$1 \cdot z = e^{i0} e^{i\theta} = e^{i(0+\theta)} = e^{i\theta} = z,$$

and similarly $z \cdot 1 = z$.

(G3) **(Inverses)** For any $z = e^{i\theta} \in S^1$, its inverse is given by $z^{-1} = e^{-i\theta}$, since

$$z \cdot z^{-1} = e^{i\theta} e^{-i\theta} = e^{i(\theta-\theta)} = e^{i \cdot 0} = 1.$$

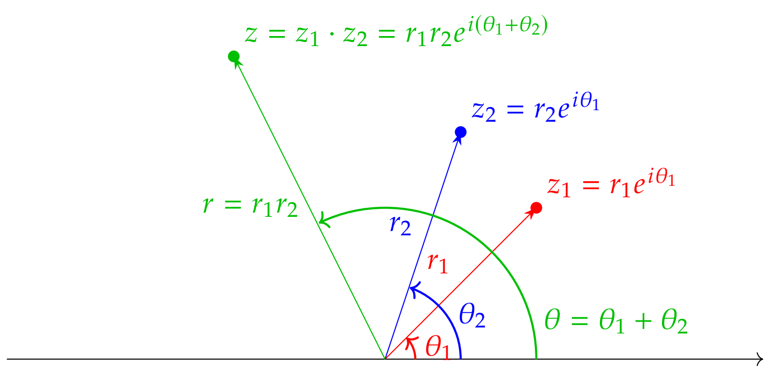
Notice that $e^{-i\theta} \in S^1$ as well.

We show that **multiplication on the circle group is equivalent to addition of angles**: let

$$\begin{aligned} z_1 &= r_1 e^{i\theta_1} = r_1 (\cos\theta_1 + i \sin\theta_1) \in \mathbb{C} \text{ and} \\ z_2 &= r_2 e^{i\theta_2} = r_2 (\cos\theta_2 + i \sin\theta_2) \in \mathbb{C}. \end{aligned}$$

Then

$$\begin{aligned} z_1 \cdot z_2 = r_1 e^{i\theta_1} \cdot r_2 e^{i\theta_2} = &= r_1 r_2 (\cos\theta_1 + i \sin\theta_1)(\cos\theta_2 + i \sin\theta_2) \\ &= r_1 r_2 \left[(\cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2) + i (\cos\theta_1 \sin\theta_2 + \sin\theta_1 \cos\theta_2) \right] \\ &= r_1 r_2 \left[\cos(\theta_1+\theta_2) + i \sin(\theta_1+\theta_2) \right] \\ &= r(\cos\theta + \sin\theta) \text{ with } \begin{cases} r = r_1 r_2 \\ \theta = \theta_1 + \theta_2. \end{cases} \end{aligned}$$



However, it is important to note that S^1 itself is not a cyclic group because no single element can generate the entire uncountable set. A group G is called **cyclic** if there exists an element $g \in G$ such that

$$G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}.$$

In the context of S^1, while the full group is not cyclic, every finite subgroup of S^1 is cyclic.

S^1 is a compact, connected, and smooth one-dimensional manifold. Its compactness follows from the Heine-Borel theorem, and its connectedness is inherent in the continuity of the circle. These topological features are critical in understanding its role as a topological group.

Though S^1 is a group under multiplication, it is not cyclic. To see this, consider any element $e^{i\theta} \in S^1$. The subgroup generated by $e^{i\theta}$ is:

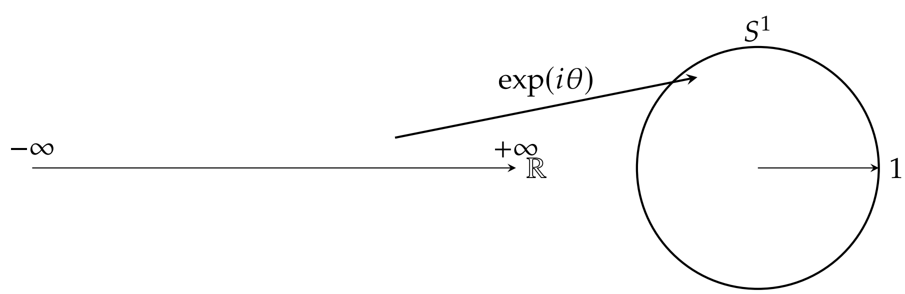
$$\langle e^{i\theta} \rangle = \{e^{in\theta} : n \in \mathbb{Z}\}.$$

If $\theta/2\pi$ is irrational, then $\langle e^{i\theta} \rangle$ is dense in S^1 but does not equal S^1 since it is countable. If $\theta/2\pi$ is rational, the subgroup is finite. In either case, no single element can generate the entire uncountable group S^1.

The exponential map provides a natural connection between the additive group $\mathbb{R}$ and the multiplicative group S^1:

$$\exp : \mathbb{R} \to S^1, \quad \exp(i\theta) = e^{i\theta}.$$

This continuous group homomorphism is essential in many areas of analysis and differential geometry.



For any positive integer n, the nth roots of unity form a finite cyclic subgroup of S^1. Specifically, define:

$$C_n = \{e^{2\pi ik/n} : k = 0, 1, \ldots, n-1\}.$$

This group is cyclic because it can be generated by the element:

$$e^{2\pi i/n},$$

and every element in C_n is a power of this generator.

The cyclic group C_n is a fundamental object in various fields:

- **Number Theory:** The nth roots of unity are closely related to cyclotomic polynomials.
- **Signal Processing:** They appear in the discrete Fourier transform (DFT).
- **Algebra:** Finite cyclic groups are among the simplest groups and serve as building blocks for more complex structures.

S^1 is not only a topological group but also a Lie group. Its smooth manifold structure enables the study of continuous group representations and provides a gateway into harmonic analysis.

The study of S^1 and its subgroups extends to many areas:

- **Differential Geometry:** S^1 serves as an example of a smooth manifold with a rich geometric structure.
- **Complex Analysis:** As the boundary of the unit disk, S^1 plays a key role in conformal mappings and function theory.
- **Algebraic Topology:** The fundamental group of S^1 is isomorphic to $\mathbb{Z}$, providing insight into covering spaces and homotopy theory.

Recall that a group G is called *cyclic* if

$$\exists\, a \in G \text{ s.t. } \forall\, g \in G,\ \exists\, n \in \mathbb{Z}:\ g = a^n.$$

Consider the circle

$$S^1 := \{\, z \in \mathbb{C} \mid |z| = 1 \,\},$$

which is a group under complex multiplication. Each element of S^1 may be written in the form

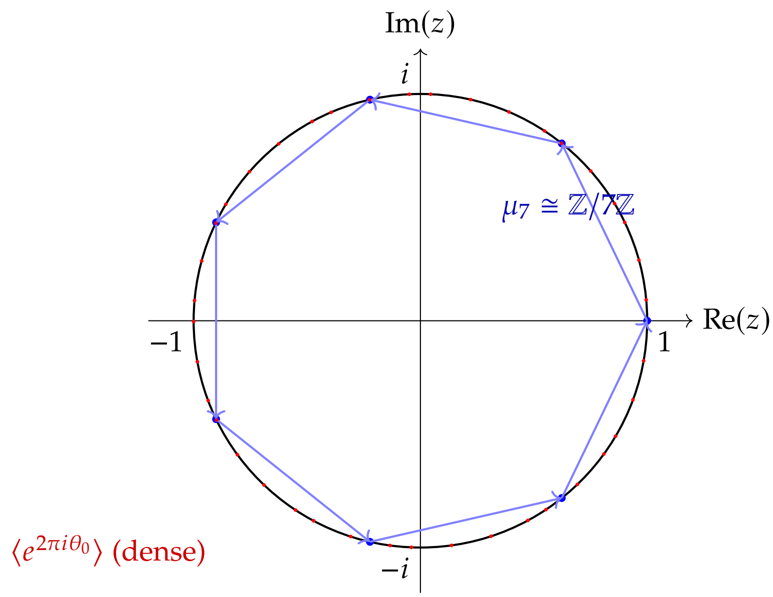
$$z = e^{2\pi i\theta}, \quad \theta \in [0,1),$$

and for a fixed irrational θ_0, the subgroup

$$\langle e^{2\pi i\theta_0} \rangle = \{\, e^{2\pi i n\theta_0} \mid n \in \mathbb{Z} \,\}$$

is dense in S^1. In the finite setting, for any $n \in \mathbb{N}$, the subgroup of nth roots of unity

$$\mu_n = \{\, e^{2\pi i k/n} \mid k = 0, 1, \ldots, n-1 \,\}$$



$S^1 = \{ z \in \mathbb{C} \mid |z| = 1 \}$

is cyclic, isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

B Torus