Abstract Algebra I

Ji, Yong-hyeon

April 6, 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. $x \cdot x^{-1} = x^{-1} \cdot x = e$.

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.

Remark. The notation a^n (or na) is understood in the group-theoretic sense,

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

The Classification for Cyclic Groups

Theorem. *Let $(G, *)$ be a cyclic group. Then*

$$(G, *) \simeq \begin{cases} (\mathbb{Z}, +) & \text{if } G \text{ is infinite,} \\ (\mathbb{Z}/n\mathbb{Z}, +_n) & \text{if } G \text{ is finite of order } n. \end{cases}$$

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 $a \in G$ be a generator of the cyclic group G, i.e., $G = \langle a \rangle$.

(*Multiplicative Version*) Define the mapping

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

Let $a, b \in \mathbb{Z}$. Then, we have

$$\varphi(a + b) = g^{a+b} = g^a * g^b = \varphi(a) * \varphi(b).$$

Thus,

$$\forall a, b \in \mathbb{Z}, \quad \varphi(a + b) = \varphi(a) * \varphi(b).$$

This shows that φ is a group homomorphism from $(\mathbb{Z}, +)$ into $(G, *)$.

(Case I) (G is infinite)

Assume that G is infinite. We claim that φ is bijective:

(i) (Surjectivity) By definition of a cyclic group, every element $h \in G$ is of the form $h = g^k$ for some $k \in \mathbb{Z}$. Hence,

$$\forall h \in G, \ \exists k \in \mathbb{Z} \text{ s.t. } \varphi(k) = g^k = h.$$

Therefore, φ is surjective.

(ii) (Injectivity) Suppose $\varphi(k) = \varphi(l)$ for some $k, l \in \mathbb{Z}$. Then

$$\begin{aligned} g^k = g^l &\implies g^{k-l} = e_G \\ &\implies k - l = 0 \\ &\implies k = l. \end{aligned}$$

Hence, φ is injective.

Thus, φ is a bijective homomorphism, and we conclude that

$$(G, *) \simeq (\mathbb{Z}, +).$$

(Case II) (G is Finite of Order n)

Now assume that G is finite and that $|G| = n$. Then by the definition of a cyclic group of finite order, there exists a minimal positive integer n such that

$$g^n = e_G.$$

We now show that for any $k, \ell \in \mathbb{Z}$,

$$g^k = g^\ell \quad \text{if and only if} \quad k \equiv \ell \pmod{n}.$$

1. **If $k \equiv \ell$ modulo n:** Then there exists an integer t such that

$$k = \ell + tn.$$

Hence,

$$g^k = g^{\ell+tn} = g^\ell * (g^n)^t = g^\ell * e_G^t = g^\ell.$$

2. **Conversely, if $g^k = g^\ell$:** Then

$$g^{k-\ell} = e_G.$$

By the minimality of n, it must be that n divides $k - \ell$; that is,

$$k - \ell = tn \quad \text{for some } t \in \mathbb{Z},$$

which precisely means $k \equiv \ell \pmod{n}$.

Thus, the relation $g^k = g^\ell$ holds if and only if k and ℓ are congruent modulo n.

This observation motivates the definition of the mapping

$$\psi : \mathbb{Z}/n\mathbb{Z} \to G, \quad \psi([k]) := g^k,$$

where $[k]$ denotes the equivalence class of k modulo n.

We now verify that ψ is a well-defined bijective homomorphism.

- **Well-defined:** If $k \equiv \ell \pmod{n}$, then as shown above, $g^k = g^\ell$. Hence, the value $\psi([k])$ does not depend on the representative chosen.

- **Homomorphism:** Let $[k], [\ell] \in \mathbb{Z}/n\mathbb{Z}$. Then

$$\psi([k] + [\ell]) = \psi([k + \ell]) = g^{k+\ell} = g^k * g^\ell = \psi([k]) * \psi([\ell]).$$

- **Surjectivity:** Every element $h \in G$ is of the form $h = g^k$ for some $k \in \mathbb{Z}$, and hence $h = \psi([k])$.

- **Injectivity:** Suppose $\psi([k]) = \psi([\ell])$; that is, $g^k = g^\ell$. Then $k \equiv \ell \pmod{n}$ by the discussion above, so $[k] = [\ell]$.

Since ψ is a well-defined bijective homomorphism, we conclude that

$$G \simeq \mathbb{Z}/n\mathbb{Z}.$$

Using only the definition of a cyclic group and elementary properties of exponents, we have shown that:

$$(G, *) \simeq \begin{cases} (\mathbb{Z}, +) & \text{if } G \text{ is infinite,} \\ (\mathbb{Z}/n\mathbb{Z}, +_n) & \text{if } G \text{ is finite of order } n. \end{cases}$$

□

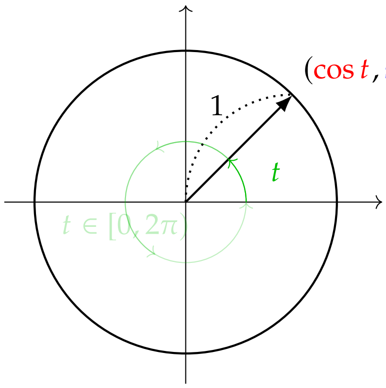
Proposition. *The subgroup of cyclic group is also cyclic.*

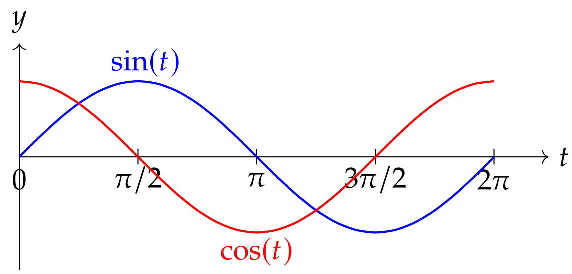
References

[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

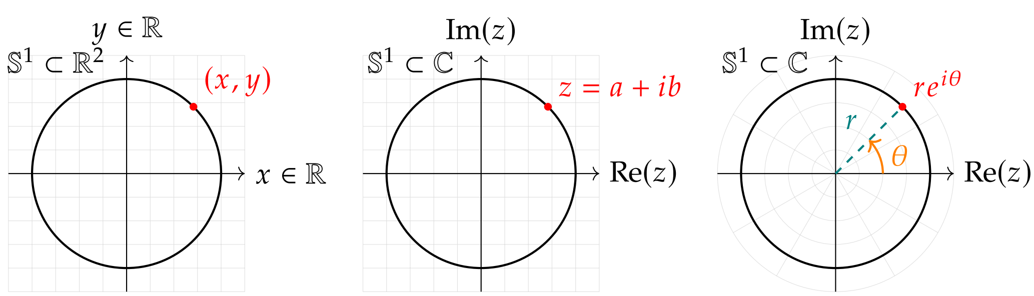
$$t \mapsto (\cos t, \sin t), \quad t \in [0, 2\pi),$$

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

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

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.



$x^2 + y^2 = 1$ $\qquad$ $|z| = 1$ $\qquad$ $|r| = 1$ 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

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

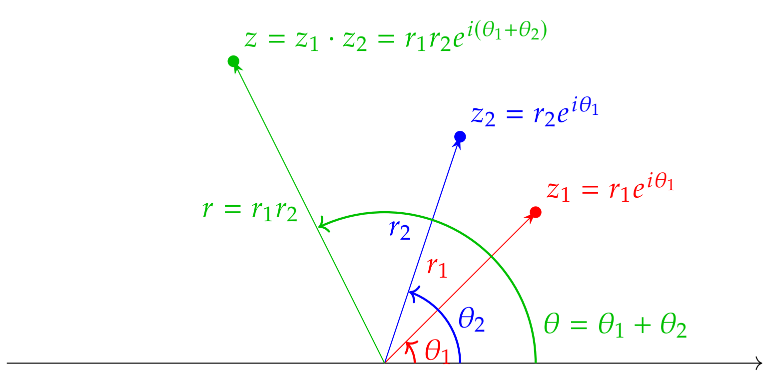
Notice that $e^{-i\theta} \in S^1$ as well.

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

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



B Torus