Abstract Algebra I

Ji, Yong-hyeon

April 7, 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

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

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

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

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

We wish to show that for all $m, n \in \mathbb{Z}$,

$$g^{m+n} = g^m * g^n.$$

Case 1. $(m, n \geq 0)$; We prove by induction on n that $g^{m+n} = g^m \cdot g^n$ for any fixed $m \geq 0$.

(i) Basic Step: $n = 0$. Since $g^0 = e$, we have:

$$g^{m+0} = g^m = g^m * e = g^m * g^0.$$

(ii) Inductive Step: Assume that for some $n \geq 0$, the statement holds; that is, $g^{m+n} = g^m * g^n$. Observe that

$$g^{m+(n+1)} = g^{(m+n)+1} = g^{m+n} * g.$$

By the induction hypothesis,

$$g^{m+n} * g = \left(g^m * g^n\right) * g.$$

By the associativity of the group operation, we can regroup the factors:

$$\left(g^m * g^n\right) * g = g^m * (g^n * g) = g^m * g^{n+1}.$$

Case 2. $m, n \leq 0$.
Let $m = -p$ and $n = -q$ with $p, q \geq 0$. Then,

$$g^{m+n} = g^{-p-q} = \left(g^{p+q}\right)^{-1}.$$

From Case 1, we know that

$$g^{p+q} = g^p \cdot g^q.$$

Taking the inverse of both sides and using the group property $(xy)^{-1} = y^{-1}x^{-1}$, we have:

$$\left(g^{p+q}\right)^{-1} = (g^p \cdot g^q)^{-1} = (g^q)^{-1} \cdot (g^p)^{-1}.$$

By definition, $(g^q)^{-1} = g^{-q}$ and $(g^p)^{-1} = g^{-p}$. Thus,

$$g^{m+n} = g^{-q} \cdot g^{-p}.$$

Since addition in the integers is commutative, we note that

$$g^m \cdot g^n = g^{-p} \cdot g^{-q} = g^{-q} \cdot g^{-p},$$

which implies $g^{m+n} = g^m \cdot g^n$ when $m, n \leq 0$.

Case 3. Mixed Signs.
Without loss of generality, assume $m \geq 0$ and $n < 0$. Write $n = -q$ with $q \geq 0$. We wish to prove:

$$g^{m-q} = g^m \cdot g^{-q}.$$

There are two subcases:

Subcase 3a: $m \geq q$.
Then $m - q \geq 0$ and from the definition of the inverse and Case 1, note that:

$$g^m = g^{(m-q)+q} = g^{m-q} \cdot g^q.$$

Multiplying on the right by $(g^q)^{-1}$ (which is g^{-q}) yields:

$$g^{m-q} = g^m \cdot (g^q)^{-1} = g^m \cdot g^{-q}.$$

Subcase 3b: $m < q$.
Then $m - q < 0$ and we write

$$g^{m-q} = \left(g^{q-m}\right)^{-1}.$$

By Case 1,

$$g^q = g^m \cdot g^{q-m}.$$

Taking inverses gives:

$$g^{-q} = \left(g^m \cdot g^{q-m}\right)^{-1} = \left(g^{q-m}\right)^{-1} \cdot (g^m)^{-1} = g^{m-q} \cdot g^{-m}.$$

Then multiplying on the right by g^m yields:

$$g^{m-q} = g^{-q} \cdot g^m.$$

In a group, although the operation need not be commutative, the definitions are set up so that the exponent law remains consistent. (A detailed handling of this subcase can be achieved by rephrasing the argument in terms of the identity $g^{q-m} = (g^{-m} \cdot g^q)^{-1}$; the result is analogous.)

Thus, in all cases, we conclude that for every $m, n \in \mathbb{Z}$,

$$g^{m+n} = g^m \cdot g^n.$$

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 ----------

(Case I) (G is infinite) Assume that G is infinite. Define the mapping

$$\varphi : (\mathbb{Z},+) \to (G,*), \quad n \mapsto \varphi(n) = \underbrace{a * \cdots * a}_{n \text{ times}} =: a^n.$$

We claim that φ is bijective homomorphism:

(i) (Homomorphism) Let $a, b \in \mathbb{Z}$. Then, we have

$$\varphi(a+b) = g^{a+b} = \underbrace{g * \cdots * g}_{a+b \text{ times}} = \underbrace{(g * \cdots * g)}_{a \text{ times}} * \underbrace{(g * \cdots * g)}_{b \text{ times}} = g^a * g^b = \varphi(a) * \varphi(b).$$

(ii) (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.

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

$$\begin{aligned} g^k = g^\ell &\implies \underbrace{g * \cdots * g}_{k \text{ times}} = \underbrace{g * \cdots * g}_{\ell \text{ times}} \\ &\implies \underbrace{g * \cdots * g}_{k \text{ times}} * \underbrace{g^{-1} * \cdots * g^{-1}}_{\ell \text{ times}} = e_G \\ &\implies g^{k-\ell} = e_G \\ &\implies k - \ell = 0 \\ &\implies k = \ell. \end{aligned}$$

Let G be a group and $g \in G$. Suppose that for some integers k and l, we have

$$g^k = g^l.$$

Since every element in a group has an inverse, we can multiply both sides of the equation by g^{-l} (the inverse of g^l). That is,

$$g^k \cdot g^{-l} = g^l \cdot g^{-l}.$$

By the definition of an inverse, we know that $g^l \cdot g^{-l} = e$, the identity element in G. Also, by the laws of exponents in groups,

$$g^k \cdot g^{-l} = g^{k-l}.$$

Thus, we obtain

$$g^{k-l} = e.$$

Hence, φ is injective.

Thus, φ is a bijective homomorphism, i.e., $(G, *) \simeq (\mathbb{Z}, +)$.

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

Now assume that G is finite, say, $|G| = n$. 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 $k, \ell \in \mathbb{Z}$,

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

($\Rightarrow$) Let $g^k = g^\ell$. 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 $k \equiv \ell \pmod{n}$.

($\Leftarrow$) Conversely, let $k \equiv \ell \pmod{n}$. Then

$$\exists t \in \mathbb{Z} \quad \text{such that} \quad k = \ell + tn.$$

Hence,

$$\begin{aligned} g^k = g^{\ell+tn} = g^\ell * (g^n)^t = g^\ell * e_G^t \\ = \underbrace{g * \cdots * g}_{\ell \text{ times}} * \underbrace{e_G * \cdots * e_G}_{t \text{ times}} \\ = g^\ell. \end{aligned}$$

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

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

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

where $[k]$ denotes the equivalence class of k modulo n, that is, $[k] = \{\ell \in \mathbb{Z} : \ell \equiv k \pmod{n}\}$. We NTS that ψ is a bijective homomorphism:

(i) (Homomorphism) Let $[k], [\ell] \in \mathbb{Z}/n\mathbb{Z}$. Then

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

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

$$\forall h \in G, \ \exists [k] \in \mathbb{Z}/n\mathbb{Z} \text{ s.t. } \psi([k]) = g^k = h.$$

Therefore, ψ is surjective.

(iii) (Injectivity) Suppose $\psi([k]) = \psi([\ell])$ for some $[k], [\ell] \in \mathbb{Z}/n\mathbb{Z}$. That is, $g^k = g^\ell$. Then $k \equiv \ell \pmod{n}$, and so $[k] = [l]$.

---------- Additive Version ----------

(Case I) (G is infinite) Assume that G is infinite. Define the mapping

$$\varphi : (\mathbb{Z}, +) \to (G, *), \quad n \mapsto \varphi(n) = \underbrace{a * \cdots * a}_{n \text{ times}} =: na.$$

We claim that φ is bijective homomorphism:

(i) (Homomorphism) Let $a, b \in \mathbb{Z}$. Then, we have

$$\varphi(a + b) = g^{a+b} = \underbrace{g * \cdots * g}_{a+b \text{ times}} = \underbrace{(g * \cdots * g)}_{a \text{ times}} * \underbrace{(g * \cdots * g)}_{b \text{ times}} = ag * bg = \varphi(a) * \varphi(b).$$

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

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

Therefore, φ is surjective.

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

$$\begin{aligned} kg = lg &\implies (k-l)g = e_G \\ &\implies k - l = 0 \\ &\implies k = l. \end{aligned}$$

Hence, φ is injective.

Thus, φ is a bijective homomorphism, i.e., $(G, *) \simeq (\mathbb{Z}, +)$.

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

Now assume that G is finite, say, $|G| = n$. 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 $k, \ell \in \mathbb{Z}$,

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

($\Rightarrow$) Let $g^k = g^\ell$. 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 $k \equiv \ell \pmod{n}$.

($\Leftarrow$) Conversely, let $k \equiv \ell \pmod{n}$. Then

$$\exists t \in \mathbb{Z} \quad \text{such that} \quad k = \ell + tn.$$

Hence,

$$\begin{aligned} g^k = g^{\ell+tn} = g^\ell * (g^n)^t = g^\ell * e_G^t &= \underbrace{g * \cdots * g}_{\ell \text{ times}} * \underbrace{e_G * \cdots * e_G}_{t \text{ times}} \\ &= g^\ell. \end{aligned}$$

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

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

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

where $[k]$ denotes the equivalence class of k modulo n, that is, $[k] = \{\ell \in \mathbb{Z} : \ell \equiv k \pmod{n}\}$. We NTS that ψ is a bijective homomorphism:

(i) (Homomorphism) Let $[k], [\ell] \in \mathbb{Z}/n\mathbb{Z}$. Then

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

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

$$\forall h \in G,\ \exists [k] \in \mathbb{Z}/n\mathbb{Z} \text{ s.t. } \psi([k]) = g^k = h.$$

Therefore, ψ is surjective.

(iii) (Injectivity) Suppose $\psi([k]) = \psi([\ell])$ for some $[k], [\ell] \in \mathbb{Z}/n\mathbb{Z}$. That is, $g^k = g^\ell$. Then $k \equiv \ell \pmod{n}$, and so $[k] = [l]$.

Hence, we conclude 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.