Abstract Algebra I

Ji, Yong-hyeon

April 16, 2025

We cover the following topics in this note.

- Cyclic Group
- Classification of Cyclic Group
- Order of an Element
- Converge of Lagrange's Theorem
- Coset
- Lagrange's Theorem

Contents

Cyclic Group and its Classification

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,

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

Note that for all $m, n \in \mathbb{Z}$,

$$g^{m+n} = g^m * g^n \quad (\text{or } (m+n)g = mg * ng).$$

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 $g \in G$ be a generator of the cyclic group G, and let e be the identity of G.

`---------------------------- Multiplicative Notation ----------------------------`

Case 1. (G is infinite) Assume that G is infinite. Define the mapping

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

We claim that φ is bijective homomorphism:

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

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

(ii) (Injectivity) Let $k, \ell \in \mathbb{Z}$. Then

$$\begin{aligned} \varphi(k) = \varphi(\ell) &\implies g^k = g^\ell \quad \text{by definition of } \varphi \\ &\implies g^k * (g^{-1})^\ell = e \\ &\implies g^k * g^{-\ell} = e \\ &\implies g^{k+(-\ell)} = e \\ &\implies k + (-\ell) = 0 \\ &\implies k = \ell. \end{aligned}$$

(iii) (Surjectivity) Let $x \in G$. Then $\exists k \in \mathbb{Z}$ such that $x = g^k$, and so

$$\varphi(k) = g^k = x.$$

Therefore, φ is surjective.

By (i), (ii) and (iii), we concluded that φ is a isomorphism, i.e., $(G,*) \simeq (\mathbb{Z},+)$.

Case 2. (G is Finite of Order n) Now assume that G is finite, say, $|G| = n \in \mathbb{N}$. Define a set

$$S := \left\{ n \in \mathbb{Z}_{\geq 0} : g^n = e \right\}.$$

Clearly $0 \in S$; that is, $S \neq \varnothing$. By well-ordering principle, $\exists n_0 = \min S$.

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 $g^{k-\ell} = e$. By the minimality of n, we know that $n \mid k - \ell$, which precisely means $k \equiv \ell \pmod{n}$.

($\Leftarrow$) Conversely, let $k \equiv \ell \pmod{n}$. Then $\exists t \in \mathbb{Z}$ such that $k = \ell + tn$, and so

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

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 $[k]$ is the equivalence class of k modulo n:

$$[k] := \left\{ \ell \in \mathbb{Z} : \ell \equiv k \pmod{n} \right\} = \left\{ \ell \in \mathbb{Z} : n \mid k - \ell \right\}$$

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

$$\psi([k]) = \psi([\ell]) \implies g^k = g^\ell \implies k \equiv \ell \pmod{n} \implies [k] = [\ell].$$

(iii) (Surjectivity) Let $x \in G$. Then $\exists k \in \mathbb{Z}$ such that $x = g^k$, and so

$$\psi([k]) = g^k = x.$$

Therefore, ψ is surjective.

By (i), (ii) and (iii), we concluded that φ is a isomorphism, i.e., $(G, *) \simeq (\mathbb{Z}/n\mathbb{Z}, +)$.

------------------------------- Additive Notation -------------------------------

Case 1. (G is infinite) Assume that G is infinite. Define the mapping

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

We claim that φ is bijective homomorphism:

(i) (Homomorphism) Let $a, b \in \mathbb{Z}$. Then, we have $\varphi(a+b) = (a+b)g = ag * bg = \varphi(a) * \varphi(b)$.

(ii) (Injectivity) Let $k, \ell \in \mathbb{Z}$. Then

$$\begin{aligned}\varphi(k) = \varphi(\ell) \implies kg = \ell g \implies kg * \ell(-g) = e &\implies kg * (-\ell)g = e \\ &\implies (k + (-\ell))g = e \\ &\implies k + (-\ell) = 0 \\ &\implies k = \ell.\end{aligned}$$

(iii) (Surjectivity) Let $x \in G$. Then $\exists k \in \mathbb{Z}$ such that $x = kg$, and so $\varphi(k) = kg = x$.

By (i), (ii) and (iii), we concluded that φ is a isomorphism, i.e., $(G, *) \simeq (\mathbb{Z}, +)$.

Case 2. (G is Finite of Order n) Now assume that G is finite, say, $|G| = n$. Define a set $S := \{n \in \mathbb{Z}_{\geq 0} : g^n = e\}$. Clearly $0 \in S$; that is, $S \neq \varnothing$. By WOP, $\exists n_0 = \min S$. Note that

$$kg = \ell g \quad \text{if and only if} \quad n \mid k - \ell.$$

Define the mapping

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

where $[k] := \{\ell \in \mathbb{Z} : n \mid k - \ell\}$. We NTS that ψ is a bijective homomorphism:

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

$$\psi([k] + [\ell]) = \psi([k + \ell]) = (k + \ell)g = kg * \ell g = \psi([k]) * \psi([\ell]).$$

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

$$\psi([k]) = \psi([\ell]) \implies kg = \ell g \implies n \mid k - \ell \implies [k] = [\ell].$$

(iii) (Surjectivity) Let $x \in G$. Then $\exists k \in \mathbb{Z}$ such that $x = g^k$, and so $\psi([k]) = g^k = x$.

By (i), (ii) and (iii), we concluded that φ is a isomorphism, i.e., $(G, *) \simeq (\mathbb{Z}/n\mathbb{Z}, +)$. □

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

Proof. Suppose G is a cyclic group. Then, by definition, $\exists g \in G$ such that

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

Let $H \leq G$. We consider two cases:

Case 1. Let H is the trivial subgroup; that is, $H = \{e\}$. Clearly $H = \{e\} = \langle e \rangle$.
Case 2. Let H is nontrivial subgroup; that is, $H \neq \{e\}$.

Since $H \leq G$ and G is cyclic, for each $h \in H$, $\exists k \in \mathbb{Z}$ s.t. $h = g^k$. Define the set

$$S = \{k \in \mathbb{Z}_{\geq 0} : g^k \in H\}.$$

Since H is nontrivial, $S \neq \varnothing$. By the well-ordering principle,

$$\exists m = \min\{k \in \mathbb{Z}_{\geq 0} : g^k \in H\}, \quad \text{so that } g^m \in H.$$

We claim that $H = \langle g^m \rangle$:

($H \supseteq \langle g^m \rangle$) Let $a \in \langle g^m \rangle$. Then $\exists k \in \mathbb{Z}$ such that $a = (g^m)^k$. Since $g^m \in H$ and $H \leq G$,

$$a = (g^m)^k = \underbrace{g^m * \cdots * g^m}_{k \text{ factors}} \in H.$$

($H \subseteq \langle g^m \rangle$) Let $h \in H$. By the Division Algorithm, $\exists! q, r \in \mathbb{Z}$ such that

$$k = qm + r, \quad 0 \leq r < m.$$

Then $g^k = g^{qm+r} = g^{qm} * g^r = (g^m)^q * g^r$, and so

$$g^r = g^k * (g^m)^{-q} \in H \overset{m=\min S}{\Longrightarrow} r = 0 \implies h = g^{qm} = (g^m)^q \implies h \in \langle g^m \rangle.$$

In either case, H is cyclic. Hence it is proved. □

Theorem. *Every cyclic group is abelian.*

The Converge of Lagrange's Theorem for Finite Cyclic Groups

Order of an Element

Definition. Let $(G, *)$ be a group. For any $g \in G$, we define the set

$$\left\{n \in \mathbb{N} : g^n = e\right\},$$

The **order of g**, denoted by $\operatorname{ord}(g)$, is defined by

$$\operatorname{ord}(g) := \begin{cases} \min\left\{n \in \mathbb{N} : g^n = e\right\} & : \varnothing \neq \left\{n \in \mathbb{N} : g^n = e\right\} \\ \infty & : \varnothing = \left\{n \in \mathbb{N} : g^n = e\right\} \end{cases}$$

That is, if there exists at least one positive integer $n \in \mathbb{N}$ such that g^n, then $\operatorname{ord}(g)$ is the smallest such n; otherwise, we say that g has infinite order and write $\operatorname{ord}(g) = \infty$.

Remark (Specialization to Cyclic Groups.)**.** Let G is a cyclic group. Then $\exists g \in G$ such that

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

- If G is infinite, then no positive integer n satisfies $g^n = e$, so $\left\{n \in \mathbb{N} : g^n = e\right\} = \varnothing$ and consequently $\operatorname{ord}(g) = \infty$.
- If G is finite of order n, then by *Lagrange's Theorem*[1] the unique smallest positive integer n for which $g^n = e$ must divide $|G|$, and in the case where g is a generator, $\operatorname{ord}(g) = n = |G|$.

Remark. Let $x \in G$ be an element of a cyclic group G with finite order $n = \operatorname{ord}(x)$. Then

$$\boxed{x^m = e \iff n \mid m \quad \text{for any } m \in \mathbb{Z}}.$$

($\Rightarrow$) By the Division Algorithm, $\exists! q, r$ s.t. $m = nq + r$ and $0 \le r < n$. Then

$$x^m = x^{nq+r} = x^{nq} * x^r = (x^n)^q * x^r = e^q * x^r = x^r.$$

Since $x^m = e$, we have

$$x^r = e \quad \text{with} \quad 0 \le r < n.$$

However, by the minimality of $n = \operatorname{ord}(x)$, r must be 0. Thus, $m = nq$, i.e., $n \mid m$.

($\Leftarrow$) $n \mid m \implies \exists q \in \mathbb{Z} : m = nq \implies x^m = x^{nq} = (x^n)^q = e^q = e.$

[1] If G be a finite group and $H \le G$, then $|H|$ divides $|G|$. In this context, $|\langle g \rangle| = \operatorname{ord}(g)$ divides $|G| = n$.

Lagrange's Theorem

Theorem. *Let G be a finite group and let $H \leq G$ be a subgroup. Then $|H|$ divides $|G|$.*

Proof. In this note, we prove it at the end. □

Division Algorithm

Theorem. *Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}_{>0}$. Then there exists unique integers q and r such taht*

$$a = qb + r \quad \textit{and} \quad 0 \leq r < b.$$

Proof. It is proved by well-ordering principle. □

Lemma. *Let G be a cyclic group and let $x \in G$ with $\operatorname{ord}(x) = n \in \mathbb{N}$. Then, for each $a \in \mathbb{Z}$,*

$$\boxed{\operatorname{ord}(x^a) = \frac{n}{\gcd(n,a)}}.$$

Proof. Note that

$$\operatorname{ord}(x^a) := \min\left\{k \in \mathbb{N} : (x^a)^k = e\right\} = \min\left\{k \in \mathbb{N} : n \mid ak\right\}.$$

Let $\operatorname{ord}(x^a) =: t \in \mathbb{Z}$; that is, $(x^a)^t = e$. Consider $d := \gcd(n,a) \in \mathbb{N}$. Then $d \mid n$ and $d \mid a$, and so

$$\exists k_n, k_a \in \mathbb{Z} \text{ such that } n = dk_n \text{ and } a = dk_a,$$

with $\gcd(k_n, k_a) = \gcd\left(\frac{n}{d}, \frac{a}{d}\right) = 1$. And then

$$\begin{aligned}(x^a)^t = e \implies n \mid at \implies dk_n \mid (dk_a)t &\implies k_n \mid k_a t \\ &\implies k_n \mid t \quad \text{by Euclid's Lemma.}\end{aligned}$$

Since

$$(x^a)^{k_n} = (x^{dk_a})^{k_n} = (x^{dk_n})^{k_a} = (x^n)^{k_a} = e$$

and the minimality of $t = \operatorname{ord}(x^a)$, k_n must t, i.e., $k_n = t$. Thus,

$$\operatorname{ord}(x^a) = t = k_n = \frac{n}{d} = \frac{n}{\gcd(n,a)}.$$

□

The Converse of Lagrange's Theorem for Finite Cyclic Groups

Theorem. *Let G be a finite cyclic group with $|G| = n$. Then for each $d \in \mathbb{N}$ with $d \mid n$,*

$$\exists! H \leq G \text{ such that } |H| = d.$$

Proof. Since G is cyclic, $\exists x \in G$ such that

$$G = \langle x \rangle = \left\{ x^k : k \in \mathbb{Z} \right\}.$$

Since $n = |G| = |\langle x \rangle|$, we have

$$x^n = e \quad \text{and} \quad n = \operatorname{ord}(x) = \min \left\{ k \in \mathbb{N} : x^k = e \right\}.$$

Let $d \in \mathbb{N}$ be a divisor of n; that is $d \mid n$. Then $\exists m \in \mathbb{N}$ such that $n = dm$.

(Existence) Define the element

$$y := x^m = x^{\frac{n}{d}} \in G$$

We claim that the subgroup generated by y, $H := \langle y \rangle$, has order d; that is $\operatorname{ord}(y) = d$. Note that

$$H = \langle y \rangle = \left\{ y^k : k \in \mathbb{Z} \right\} = \left\{ (x^m)^k : k \in \mathbb{Z} \right\}.$$

Here, let k be the smallest positive integer k such that $y^k = e$. Then

$$y^k = e \implies x^{mk} = e \implies n \mid mk \implies dm \mid mk \implies d \mid k.$$

Since $y^d = (x^m)^d = x^{md} = x^n = e$ and k is the *smallest* positive integer with this property, thus,

$$\operatorname{ord}(y) = k = d.$$

(Uniqueness) Let

$$K \leq G = \langle x \rangle = \left\{ x^k : k \in \mathbb{Z} \right\}.$$

with $|K| = d$. That is, $\exists \ell \in \mathbb{Z}$ such that $K = \langle x^\ell \rangle$. Then

$$\operatorname{ord}(x^\ell) = \frac{n}{\gcd(n, \ell)} = d,$$

so that $\gcd(n, \ell) = \dfrac{n}{d}$. By Bézout's identity,

$$\exists r, s \in \mathbb{Z} \quad \text{and} \quad rn + s\ell = \gcd(n, \ell) = \frac{n}{d}.$$

Then

$$\begin{aligned} x^{rn+s\ell} &= x^{n/d}, \\ (x^n)^r * x^{s\ell} &= x^{n/d}, \\ x^{s\ell} &= x^{n/d}, \\ (x^\ell)^s &= x^{n/d}. \end{aligned}$$

Hence

$$K = \langle x^\ell \rangle = \langle x^{n/d} \rangle = H.$$

$\square$

Euler's Phi Function

Definition. The **Euler's Phi Function** $\phi : \mathbb{Z} \to \mathbb{Z}$ is defined by

$$\varphi(n) := \begin{cases} \#\left\{k \in \{1,2,\ldots,|n|\} : \gcd(k,|n|) = 1\right\} & : n \neq 0, \\ 0 & : n = 0. \end{cases}$$

We set $\varphi(0) = 0$ by convention.

Remark. Consider a cyclic group $\mathbb{Z}/n\mathbb{Z}$ of order n (under $+_n$). Recall that, for $[a] \in \mathbb{Z}/n\mathbb{Z}$,

$$\operatorname{ord}([a]) = \frac{n}{\gcd(a,n)}.$$

Here, if $\gcd(a,n) = 1$ then $\operatorname{ord}([a]) = n$; that is, $[a]$ be a generator of $\mathbb{Z}/n\mathbb{Z}$. Thus, the set of generators of $\mathbb{Z}/n\mathbb{Z}$ is

$$\{\, [a] \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1 \,\},$$

and so

$$\varphi(n) = \#\{\, a \in \{1,2,\ldots,n\} : \gcd(a,n) = 1 \,\},$$

which is precisely the number of generators of $\mathbb{Z}/n\mathbb{Z}$.

Properties of Euler-Phi Function

Proposition. *Let $p \in \mathbb{N}_{>1}$ be a prime, and let $k, m, n \in \mathbb{Z}$. Then*

(1) $\varphi(p^k) = p^k - p^{k-1}$.

(2) $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. Consider a prime p and let $k, m, n \in \mathbb{N}$.

(1) The Euler's phi function counts the number of $a \in [1, p^k]$ that are coprime to p^k:

$$\varphi(p^k) = \#\{\, a \in \{1, 2, \ldots, p^k\} : \gcd(a, p^k) = 1 \,\}.$$

The multiples of p in $\{1, 2, \ldots, p^k\}$ is

$$1 \cdot p, \quad 2 \cdot p, \quad \cdots, \quad p^{k-1}(= p^{k-2} \cdot p), \quad p^k(= p^{k-1} \cdot p),$$

and so its number is precisely p^{k-1}. Thus,

$$\varphi(p^k) = p^k - p^{k-1}.$$

(2) TBA

□

Coset and Lagrange's Theorem

Observation (Group $\mathbb{Z}$ and subgroup $n\mathbb{Z}$). Consider an abelian group $(\mathbb{Z}, +)$. For a fixed $n \in \mathbb{Z}\backslash\{0\}$, we define

$$n\mathbb{Z} := \{\underbrace{n + \cdots + n}_{k \text{ factors}} : k \in \mathbb{Z}\} = \{nk : k \in \mathbb{Z}\}.$$

Note that $0 \in n\mathbb{Z}$ since $0 = n \cdot 0$. Thus, $n\mathbb{Z}$ is nonempty. Let $a, b \in n\mathbb{Z}$ then

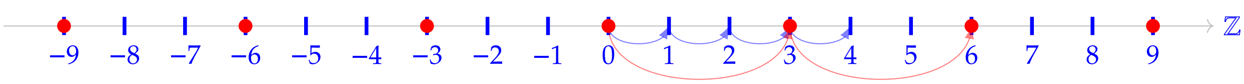
$$\exists k, \ell \in \mathbb{Z} \quad \text{such that} \quad a = nk \text{ and } b = n\ell.$$

Then

$$\begin{aligned} a + (-b) &= nk + n(-\ell) \\ &= n(k + (-\ell)) \\ &\in n\mathbb{Z} \quad \because k + (-\ell) \in \mathbb{Z}. \end{aligned}$$

Thus, $(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$. Note that $n\mathbb{Z}$ is a "grid" inside $\mathbb{Z}$:

$$3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\} = \{\underbrace{3 + \cdots + 3}_{k \text{ factors}} \mid k \in \mathbb{Z}\}$$

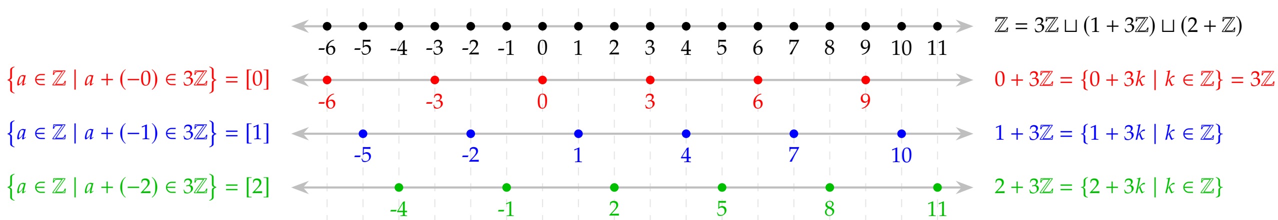


Observation (Partition via the Division Algorithm). Let $n \in \mathbb{Z} \setminus \{0\}$. Given any $a \in \mathbb{Z}$, the Division Algorithm guarantees that $\exists! q, r \in \mathbb{Z}$ such that

$$a = nq + r, \quad \text{with } 0 \leq r < n.$$

This leads to the relation $a - r = nq$, i.e., $a - r \in n\mathbb{Z}$. Consequently, we say that

$$a + (-r) \in n\mathbb{Z} \iff n \mid a + (-r) \iff a \equiv r \pmod{n}.$$



Hence, one may assign to each $a \in \mathbb{Z}$ the corresponding set

$$\begin{aligned} a + n\mathbb{Z} &= (nq + r) + n\mathbb{Z} \\ &= (r + nq) + n\mathbb{Z} \\ &= r + n\mathbb{Z} = \{r + nk : k \in \mathbb{Z}\}. \end{aligned}$$

The set of all integers is the disjoint union of these residue classes: $\mathbb{Z} = \bigsqcup_{r=0}^{n-1} (r + n\mathbb{Z})$.

Note.

Group	$(\mathbb{Z}, +)$		$(G, *)$
Subroup	$(n\mathbb{Z}, +) \leq (\mathbb{Z}, +)$		$(H, *) \leq (G, *)$
Relation	$a \sim r \Leftrightarrow a + (-r) \in n\mathbb{Z}$	$\xrightarrow{\text{Generalization}}$	$g_1 \sim g_2 \Leftrightarrow g_1 * g_2^{-1} \in H$
Coset	$a + n\mathbb{Z} = \{a + nk : k \in \mathbb{Z}\}$		$g * H := \{g * h : h \in H\}$
Quotient Group with Operation	$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} : a \in \mathbb{Z}\}$ with $(a + n\mathbb{Z}) \boxplus (b + n\mathbb{Z}) := (a + b) + n\mathbb{Z}$		$G/H := \{g * H : g \in G\}$ with $(g_1 * H) \boxast (g_2 * H) := (g_1 * g_2) * H$
Partition	$\mathbb{Z} = \bigsqcup_{r=0}^{n-1} (r + n\mathbb{Z})$		$G = \bigsqcup_{g \in G} (g * H)$

Proposition. *Let $(G, *)$ be a group and $H \leq G$. Define a binary relation $\sim_L$ and $\sim_R$ on G by*

$$g_1 \sim_L g_2 \iff g_1^{-1} * g_2 \in H,$$
$$g_1 \sim_R g_2 \iff g_1 * g_2^{-1} \in H.$$

Then $\sim_L$ and $\sim_R$ are both equivalence relations on G.

Proof. We NTS that a relation $\sim_L$ on G is reflexive, symmetric and transitive:

(i) (Reflexivity) Take $g \in G$. Note that $g^{-1} * g = e$ is the identity element of G. Since H is a subgroup, it must contain e. Thus, $g^{-1} * g = e \in H$, i.e., $g \sim_L g$.

(ii) (Symmetry) Let $g_1, g_2 \in G$. Suppose that $g_1 \sim_L g_2$; that is, $g_1^{-1} * g_2 \in H$. Since H is a subgroup,

$$g_2^{-1} * g_1 = (g_1^{-1} * g_2)^{-1} \in H, \quad \text{i.e.,} \quad g_2 \sim_L g_1.$$

(iii) (Transitivity) Let $g_1, g_2, g_3 \in G$. Suppose that $g_1 \sim_L g_2$ and $g_2 \sim_L g_3$; that is, $g_1^{-1} * g_2, g_2^{-1} * g_3 \in H$. Since $H \leq G$,

$$g_1^{-1} * g_3 = g_1^{-1} * (g_2 * g_2^{-1}) * g_3 = (g_1^{-1} * g_2) * (g_2^{-1} * g_3) \in H, \quad \text{i.e.,} \quad g_1 \sim_L g_3.$$

Hence, $\sim_L$ is equivalence relations on G and similarly $\sim_R$ is also. □

Coset

Definition. Let $(G, *)$ be a group with identity element e, and let $H \leq G$ be a subgroup of G. For any element $g \in G$, the **left coset** of H in G corresponding to g is defined by

$$g * H := \{ g * h : h \in H \} \subseteq G.$$

Similarly, the **right coset** of H in G corresponding to g is defined by $H * g := \{ h * g : h \in H \}$.

Remark. Note that
$$x \in g * H \iff \exists h \in H; \text{such that } x = g * h.$$

Thus, $H = e * H = H * e$ since $h = e * h = h * e$ for any $h \in H$.

Remark. Consider the equivalence relation $\sim_L$ on G. For each $g \in G$, we obtain

$$[g] = \left\{x \in G : g \sim_L x\right\} = \left\{x \in G : g^{-1} * x \in H\right\} = \left\{g * h : h \in H\right\} = gH.$$

Coset Equality Criterion

Proposition. *Let G be a group and let $H \le G$ be a subgroup. Then, for all $g_1, g_2 \in G$, the following conditions are equivalent:*

(1) $g_1 * H = g_2 * H$

(2) $g_1^{-1} * g_2 \in H$

(3) $g_2^{-1} * g_1 \in H$.

Proof. Let $g_1, g_2 \in G$.

[(1)⇒(2)] Assume that $g_1 * H = g_2 * H$. Then

$$\begin{aligned} g_2 = g_2 * e \implies g_2 \in g_2H = g_1H &\implies \exists h \in H \text{ s.t. } g_2 = g_1 * h \\ &\implies g_1^{-1} * g_2 = h \in H. \end{aligned}$$

[(2)⇒(1)] Assume that $g_1^{-1} * g_2 \in H = e * H$. Then

$$\exists h \in H \text{ such that } g_1^{-1} * g_2 = e * h = h, \text{ i.e., } g_2 = g_1 * h.$$

(a) ($g_1H \supseteq g_2H$) Let $y \in g_2 * H$ then $\exists h' \in H$ such that $y = g_2 * h'$. Thus

$$y = g_2 * h' = (g_1 * h) * h' = g_1 * (h * h') \overset{h*h' \in H}{\in} g_1H.$$

(b) ($g_1H \subseteq g_2H$) Let $x \in g_1 * H$ then $\exists h'' \in H$ such that $x = g_1 * h''$. Thus

$$x = g_1 * h'' = (g_2 * h^{-1}) * h'' = g_2 * (h^{-1} * h'') \overset{h^{-1}*h' \in H}{\in} g_2 * H.$$

By (a) and (b), we obtain that $g_1 * H = g_2 * H$.

[(2)⇔(3)] Note that $(g_1^{-1}g_2)^{-1} = g_2^{-1}g_1$. Since H is a subgroup, we have

$$g_1^{-1}g_2 \in H \iff (g_1^{-1}g_2)^{-1} \in H \iff g_2^{-1}g_1 \in H.$$

□

Equal Cardinalities of Cosets

Proposition. *Let $(G, *)$ be a group, and let $H \leq G$. Then*

$$|g * H| = |H|, \quad \text{for all } g \in G.$$

Proof. Let $g \in G$. Define a mapping

$$\varphi : H \to g * H, \quad h \mapsto \varphi(h) := g * h.$$

We NTS that φ is a bijection:

(i) (Injectivity) Let $h_1, h_2 \in H$. Then

$$\begin{aligned} \varphi(h_1) = \varphi(h_2) &\implies g * h_1 = g * h_2 \\ &\implies g^{-1} * (g * h_1) = g^{-1} * (g * h_2) \\ &\implies h_1 = h_2. \end{aligned}$$

(ii) (Surjectivity) Let $x \in g * H$. Then $\exists h \in H$ such that $x = g * h$, and so

$$\varphi(h) = g * h = x.$$

Hence it is proved. □

Quotient Group G/H

Definition. Let G be a group and let H be a normal subgroup of G (that is, $g * H * g^{-1} = H$ for all $g \in G$). The **quotient group** G/H is defined by

$$G/H := \left\{g * H : g \in G\right\},$$

where for each $g \in G$, the *left coset* $g * H$ is the set

$$g * H := \left\{g * h : h \in H\right\}.$$

The binary operation on G/H is defined by

$$(g_1 * H) \boxtimes (g_2 * H) := (g_1 * g_2) * H, \quad \text{for all } g_1, g_2 \in G.$$

Exercise. Prove that there exists a group isomorphism from $G/\{e\}$ to G.

Sol. The set of left cosets of $\{e\}$ in G is $G/\{e\} = \left\{g * \{e\} : g \in G\right\}$. Define a function

$$\varphi : G/\{e\} \to G, \quad g * \{e\} \mapsto \varphi(g * \{e\}) := g.$$

Then

(i) (Well-definedness) Let $g * \{e\} = h * \{e\}$ for some $g, h \in G$. Then

$$h^{-1} * g \in \{e\} \implies h^{-1} * g = e \implies g = h.$$

(ii) (Homomorphism) Let $g * \{e\}, h * \{e\} \in G/\{e\}$. Then

$$\varphi((g * \{e\}) \boxtimes (h * \{e\})) = \varphi((g * h) * \{e\}) = g * h = \varphi(g * \{e\}) * \varphi(h * \{e\})$$

(iii) (Injectivity) $\varphi(g * \{e\}) = \varphi(h * \{e\}) \implies g = h \implies g * \{e\} = h * \{e\}$.

(iv) (Surjectivity) Let $g \in G$. Then $\exists g * \{e\} \in G/\{e\}$ such that $\varphi(g * \{e\}) = g$.

□

Lagrange's Theorem

Theorem. *Let $(G, *)$ be a finite group and let $H \leq G$ be a subgroup. Then*

$$|H| \quad \textit{divides} \quad |G|.$$

Proof. Consider equivalence classes (left cosets) be denoted by

$$g_1H,\ g_2H,\ \ldots,\ g_kH,$$

where $k \in \mathbb{N}$. Since $G = \bigsqcup_{i=1}^{k} g_iH$, we have

$$\begin{aligned} |G| &= \sum_{i=1}^{k} |g_iH| \\ &= \sum_{i=1}^{k} |H| \quad \because |g_iH| = |H| \quad \text{for all } i = 1, 2, \ldots, k. \\ &= k \cdot |H|. \end{aligned}$$

Hence, the order (cardinality) of H divides the order of G. □

Corollary. *Let p be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ has no proper subgroup except $\{e\}$. In other words, if H is a subgroup of $\mathbb{Z}/p\mathbb{Z}$, then either*

$$H = \{[0]\} \quad \textit{or} \quad H = \mathbb{Z}/p\mathbb{Z}.$$

Proof. Consider the group $G = \mathbb{Z}/p\mathbb{Z}$. Since p is prime, we have $|G| = p$. Let $H \leq \mathbb{Z}/p\mathbb{Z}$. Then, by Lagrange's Theorem, $|H|$ must divide p. By the definition of a prime,

$$|H| \in \{1, p\}.$$

Case 1. If $|H| = 1$, then $H = \{[0]\}$.
Case 2. If $|H| = p$, then $H = \mathbb{Z}/p\mathbb{Z}$.

Thus, there is no proper nontrivial subgroup of $\mathbb{Z}/p\mathbb{Z}$; the only subgroups are the trivial subgroup and the group itself. □

Corollary. *Every group of prime order is cyclic.*

Proof. Let $|G| = p$, where p is prime. Then $|G| > 1$ and so $\exists g \in G$ with $g \neq e$. Consider $\langle g \rangle \leq G$. By Lagrange's Theorem, $|\langle g \rangle|$ divides $|G| = p$. Since p is prime, either

$$\mathrm{ord}(g) = 1 \quad \text{or} \quad \mathrm{ord}(g) = p.$$

Case 1. If $\mathrm{ord}(g) = 1$, then $G = \{e\}$. It is contradict to the $|G| > 1$.
Case 2. If $\mathrm{ord}(g) = p$, then $|G| = p = \left|\langle g \rangle\right|$.

Therefore, $G = \langle g \rangle$. □

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.

[2] 수학의 즐거움, Enjoying Math. "수학 공부, 기초부터 대학원 수학까지, 21. 추상대수학 (b) 순환군과 라그랑지 정리의 역방향 cyclic group and inverse of Lagrange theorem" YouTube Video, 32:03. Published October 19, 2019. URL: https://www.youtube.com/watch?v=_oY-2n6_xEg&t=1744s.

[3] 수학의 즐거움, Enjoying Math. "수학 공부, 기초부터 대학원 수학까지, 22. 추상대수학 (c) 잉여류와 라그랑지 정리 set of cosets and Lagrange's theorem" YouTube Video, 22:33. Published October 22, 2019. URL: https://www.youtube.com/watch?v=dsyssRBSqow&t=835s.

A Number Theory

A.1 Divisibility

Divisibility

Definition. Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Then a **divides** b if

$$\exists c \in \mathbb{Z} \quad \text{such that} \quad b = ac.$$

Then a is *divisor* or *factor* of b and b is *multiple* of a.

Remark. We write $a \mid b$ if a divides b, and $a \nmid b$ otherwise.

Remark. Let $a, b \in \mathbb{N}$. Then $a \mid b \implies a \leq b$.

Proof. Let $a \mid b$. Then

$$\exists k \in \mathbb{N} \quad \text{such that} \quad b = a \cdot k.$$

Note that $k \geq 1$. Then

$$a \cdot k \geq a \cdot 1 \implies b \geq a \cdot 1 \implies b \geq a.$$

□

Proposition. *Let $a, b, c \in \mathbb{Z}$.*

(1) $a \mid b$ and $b \mid c \implies a \mid c$.

(2) Let $c \neq 0$. Then $ca \mid cb \implies a \mid b$.

Proof. Let $a, b, c \in \mathbb{Z}$.

(1) Let $a \mid b$ and $b \mid c$. Then $\exists u, v \in \mathbb{Z}$ s.t. $au = b$ and $bv = c$. Thus

$$c = bv = (au)v = a(uv),$$

and so $a \mid c$.

(2) Let $ca \mid cb$ with $c \neq 0$. Then $\exists u \in \mathbb{Z}$ s.t. $cb = cau$. Hence $b = au$, and so $a \mid b$.

□

Proposition. *Let $a, b, c \in \mathbb{Z}$. For any $m, n \in \mathbb{Z}$,*

$$c \mid a \text{ and } c \mid b \implies c \mid (ma + nb).$$

Proof. Let $m.n \in \mathbb{Z}$, and let $a \mid b$ and $b \mid c$. Then

$$\exists e, f \in \mathbb{Z} \text{ such that } a = ce \text{ and } b = cf.$$

Hence

$$ma + nb = m(ce) + n(cf) = c(me + nf),$$

and so $c \mid (ma + nb)$. □

Euclid's Lemma

Theorem. *Let $a, b, c \in \mathbb{Z}$, and let $a \mid bc$. Then*

$$\gcd(a, b) = 1 \implies a \mid c.$$

Proof. By Bézout's Identity, $\exists a, b \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b) = 1.$$

Consider

$$c \cdot 1 = c(ax + by) = cax + cby.$$

Since $a \mid ac$ and $a \mid bc$, we have

$$a \mid (cax + cby).$$

Hence, $a \mid c$. □

A.2 Modular Arithmetic

Congruence (Number Theory)

Definition. Let n be a positive integer ($n \in \mathbb{N}$). Two integers a and b are said to be **congruent modulo** n, written as

$$a \equiv b \pmod{n},$$

if and only if

$$n \mid a - b, \quad \text{i.e.,} \quad \exists k \in \mathbb{Z} \text{ such that } a - b = kn.$$

Remark (Modulo Operation)**.** According to the **division algorithm**, for any integer a and any positive integer n, there exist unique integers q (the quotient) and r (the remainder) such that

$$a = qn + r \quad \text{with} \quad 0 \le r < n.$$

When we express this using the floor function and the mod operation, we identify:

$$q = \left\lfloor \frac{a}{n} \right\rfloor \quad \text{and} \quad r = a \bmod n.$$

Thus, we can rewrite the division algorithm as:

$$a = n \left\lfloor \frac{a}{n} \right\rfloor + (a \bmod n).$$

Thus, we have

$$a \bmod n := \begin{cases} a - n \left\lfloor \dfrac{a}{n} \right\rfloor & : n \neq 0 \\ 0 & : n = 0. \end{cases}$$

Note that

$$a \equiv b \pmod{n} \iff a \bmod n = b \bmod n.$$

A.3 Greatest Common Divisors

Greatest Common Divisor; GCD

Definition. Let $a, b \in \mathbb{Z}$. An nonnegative integer $d \in \mathbb{Z}_{\geq 0}$ is called a **greatest common divisor (gcd)** of a and b, denoted by $d = \gcd(a, b)$, if it satisfies the following two conditions:

(i) (Divisibility) $d \mid a$ and $d \mid b$.

(ii) (Maximality) For any $c \in \mathbb{Z}$,

$$c \mid a \text{ and } c \mid b \implies c \mid d.$$

Proposition. *Let $a, b, c \in \mathbb{Z}$.*

(1) $\gcd(a + cb, b) = \gcd(a, b)$.

(2) $\gcd(a, b) = d \implies \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof. TBA □

Bezout's Identity

Theorem. *Let $a, b \in \mathbb{Z}$. Then*

$$\exists m, n \in \mathbb{Z} \quad \textit{such that} \quad \gcd(a, b) = ma + mb.$$

Remark. Note that there are infinitely many such m and n.

Proof. It is proved by well-ordering principle. □

Corollary. *Let $a, b \in \mathbb{Z}$.*

$$\gcd(a, b) = 1 \implies \exists m, n \in \mathbb{Z} \ \textit{such that}\ ma + nb = 1.$$

A.4 Prime Number

Prime Number

Definition. A number $p \in \mathbb{N}_{>1}$ is **prime** if, for $m > 0$,

$$m \mid p \implies m = 1 \text{ or } m = p.$$

A number which is not prime is composite.

Remark. A number $p \in \mathbb{N}_{>1}$ is **prime** if, for $m > 0$, $m \mid p \implies m \in \{1, p\}$.