Abstract Algebra I

Ji, Yong-hyeon

April 11, 2025

We cover the following topics in this note.

- Cyclic Group
- Classification of Cyclic Group
- Order of an Element
- 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,

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

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.

```
---------------------------- Multiplicative Version ----------------------------
```

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

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

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, $[k] = \left\{\ell \in \mathbb{Z} : \ell \equiv k \pmod{n}\right\}$. 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) (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, $[k] = \left\{\ell \in \mathbb{Z} : \ell \equiv k \pmod{n}\right\}$. 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) (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.*

Theorem. *Let $(G, *)$ be a group and let $H \leq G$ be a cyclic subgroup of G. Then H is abelian.*

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

$$H = \langle g \rangle = \left\{ g^k : k \in \mathbb{Z} \right\}, \quad \text{where} \quad g^k := \begin{cases} \underbrace{g * \cdots * g}_{k \text{ factors}} & : k > 0 \\ 0 & : k = 0 \\ (g^{-1})^{-k} & : k < 0 \end{cases}.$$

Let h_1, h_2 be arbitrary. Then $\exists m, n \in \mathbb{Z}$ such that

$$h_1 = g^m \quad \text{and} \quad h_2 = g^n.$$

Thus,

$$h_1 * h_2 = g^n * g^m = g^{n+m} = g^{m+n} = g^m * g^n = h_2 * h_1.$$

□

Order of an Element

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

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

where for each $n \in \mathbb{N}$, g^n is the n-fold $*$-operation of g with itself (and by convention, $g^0 := e$). Then 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 $n \in \mathbb{Z}^+$ 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.)**.** If $(G, *)$ is a cyclic group, then $\exists g \in G$ (called a generator) 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

$$\left\{n \in \mathbb{N} : g^n = e\right\} = \varnothing \quad \text{and} \quad \text{and consequently } \operatorname{ord}(g) = \infty.$$

- 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

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

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

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

However, by definition 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] $\left|\langle g \rangle\right| = \operatorname{ord}(g)$ divides $|G| = n$.

Lagrange's Theorem

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

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

Proof. TBA □

Remark. Let G be a finite group and let $H \leq G$ be a subgroup. Then by Lagrange's Theorem,

$$\exists a \in \mathbb{Z} \text{ such that } |G| = a \cdot |H|\,.$$

The **index** of H in G, denoted by $[G : H]$, is defined by

$$[G : H] = \frac{|G|}{|H|}.$$

In other words, $|G| = [G : H] \cdot |H|\,.$

Division Algorithm

Theorem.

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. By definition of order of an element x^a, we know that

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

Since $x^{ak} = e \iff n \mid ak$, we may write

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

Let $d := \gcd(n, a) \neq 0$. Then $d \mid n$ and $d \mid a$, and so

$$\exists k_n, k_a \in \mathbb{Z} \text{ such that } n = dk_n \text{ and } a = dk_a, \qquad \text{with} \quad \gcd(k_n, k_a) = \gcd\left(\frac{n}{d}, \frac{a}{d}\right) = 1.$$

Since

$$n \mid ak \implies dk_n \mid (dk_a)k \implies k_n \mid k_a k \overset{\gcd(k_n,k_a)=1}{\implies} k_n \mid k \overset{\text{Euclid's Lemma}}{\implies} k_n = k,$$

we obtain

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

□

Remark. By above lemma, we obtain

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

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

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

and by the definition of order,

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

Let $d \in \mathbb{N}$ be a divisor of n; that is $d \mid n$, and so

$$\exists m \in \mathbb{N} \text{ such that } n = dm.$$

(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

$$\begin{aligned} y^k = e &\implies x^{mk} = e \\ &\implies n \mid mk \quad \because \operatorname{ord}(x) = n \\ &\implies dm \mid mk \\ &\implies d \mid k \quad \because m \neq 0. \end{aligned}$$

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

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

(Uniqueness) Let $K \leq G$ is any subgroup with $|K| = d$. Then

$$K = \langle x^m \rangle \quad \text{with} \quad m = \frac{n}{d}.$$

Since x is a generator of G, $\exists k \in \mathbb{Z}$ such that

$$y = x^k \quad \text{and} \quad \text{ord}(x^k) = d.$$

Then

$$\text{ord}(x^k) = \frac{n}{\gcd(n,k)} = d.$$

Thus, the subgroup of order d in G is unique. □

Remark (The Converse of Lagrange's Theorem for Finite Abelian Groups)**.** Let G be a finite abelian group and let $d \in \mathbb{N}$ with $d \mid |G|$. Then

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

Corollary. *Let $p \in \mathbb{Z}$ be a prime. Then $\mathbb{Z}/p\mathbb{Z}$ has no proper subgroup except $\{e\}$.*

Proof. TBA. □

Euler-Phi Function

Corollary. *Define a mapping*

$$\begin{array}{cccll} \varphi & : & \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & & n & \longmapsto & \varphi(n) := \#\left\{k \in \mathbb{Z} : k = 0, 1, 2, \ldots, n-1 \textit{ such that } \gcd(n,k) = 1\right\} \end{array}$$

is called the ***Euler-phi function****.*

Remark. $\varphi(n)$ is the number of generators of $\mathbb{Z}/n\mathbb{Z}$.

Properties of Euler-Phi Function

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

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

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

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 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.

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 $\exists \lambda, \mu \in \mathbb{Z}$ s.t. $a\lambda = b$ and $b\mu = c$. Hence $c = b\mu = (a\lambda)\mu = a(\lambda\mu)$, and so $a \mid c$.

(2) Let $ca \mid cb$ with $c \neq 0$. Then $\exists \lambda \in \mathbb{Z}$ s.t. $cb = ca\lambda$. Hence $b = a\lambda$, 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 $p \in \mathbb{Z}$ be a prime number and let $a, b \in \mathbb{Z}$. Then*

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

Proof. Let $p \in \mathbb{Z}$ prime and $a, b \in \mathbb{Z}$. Assume that $p \mid ab$. We NTS that

$$p \mid a \quad \text{or} \quad p \mid b.$$

Suppose that

$$p \nmid a.$$

Since p is prime and $p \nmid a$, we know that

$$\gcd(p, a) = 1.$$

By Bézout's Identity, $\exists u, v \in \mathbb{Z}$ such that $up + va = 1$. Then

$$\begin{aligned} up + va = 1 &\implies b\big(up + va\big) = b \\ &\implies upb + vab = b \\ &\implies p \mid b \quad \because p \mid ab \text{ and so } p \mid (upb + vab) \end{aligned}$$

Hence, under the assumption $p \nmid a$, we obtain

$$p \mid b.$$

Therefore, combining the two cases, we conclude:

$$p \mid ab \implies p \mid a \text{ or } p \mid b.$$

□

A.2 Modular Arithmetic

Congruence (Number Theory)

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

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

if and only if

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

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

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

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

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

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 $c \in Z$,

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

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

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

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

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.

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

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