ABSTRACT ALGEBRA

VIVATSATHORN T.

Linear Algebra (Brief)

$M\vec{x} = \vec{u} \quad :\rightarrow \quad u_i = \sum_j M_{ij} x_i$ •

$$\underset{M}{\begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix}} \underset{\vec{x}}{\begin{pmatrix} x \\ y \\ z \end{pmatrix}} = \underset{\vec{u}}{\begin{pmatrix} u \\ v \\ w \end{pmatrix}}$$

$P = NM \quad :\rightarrow \quad p_{ik} = \sum_j N_{ij} M_{jk} = (NM)_{ik} = N_{ij} M_{jk}$

ระวังสับสน บางที่หมายถึง entry a_{ij} ไม่ใช่ product.

(Einstein's notation)
Repeated index

Identity Matrix I : $I_{ij} = \delta_{ij}$ (kronecker delta)

$$\therefore \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

→ Matrix can be constructed from rows of col. vectors or cols. of row vectors

e.g. $M = (\vec{\psi}_{(1)}, \vec{\psi}_{(2)}, \vec{\psi}_{(3)}) \; ; \; \vec{\psi}_{(i)} = \begin{pmatrix} * \\ * \\ * \end{pmatrix}$

$$\therefore M = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix}$$

→ Matrix is associative, not commutative : $(AB)C = A(BC)$

$AB \neq BA$

→ Transpose : $(MN)^T = N^T M^T$

→ Trace : $\mathrm{tr}\, M = \sum_i M_{ii} = M_{ii}$ (Sum of the diagonals)

$\mathrm{tr}\, AB = \mathrm{tr}\, BA$

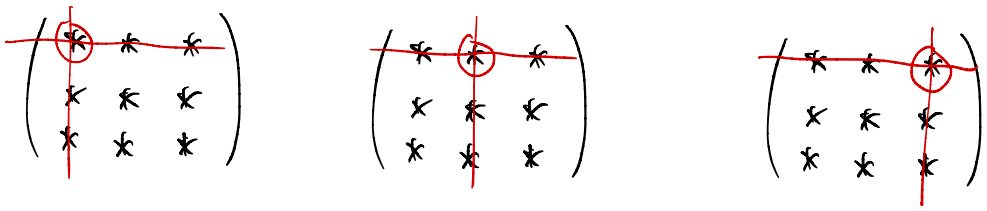
→ Inverse : $MM^{-1} = I, \quad M^{-1}M = I$

→ Scalar Matrix : $M = (a) = a$, → Null Matrix : $N = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}_{\text{any size}}$

→ Symmetric Matrix : $M^T = M$

→ Antisymmetric Matrix : $M^T = -M$
(Skew)

→ Laplace Expansion (Cofactor Expansion)



$$\det M = aC_{11} - bC_{12} + cC_{13}$$

→ Antisymmetric : Levi-Civita symbol ($\varepsilon_{\dots i_p \dots i_q \dots}$)

$$\varepsilon_{\dots i_p \dots i_q \dots} = -\varepsilon_{\dots i_q \dots i_p \dots}$$

(2D) $$\varepsilon_{ij} = \begin{cases} 1 & (i,j) = (1,2) \\ -1 & (i,j) = (2,1) \\ 0 & i = j \end{cases}$$

* Permutation Parity

$(1,3,2,4)$ is odd p. of $(1,2,3,4)$

1 (odd) swap

$(1,3,4,2)$ is even p. of $(1,2,3,4)$

2 (even) swaps

(nD) $$\varepsilon_{ij\dots} = \begin{cases} 1 & (i,j,k,\dots) \text{ is even permutation of } (1,2,3,\dots) \\ -1 & (i,j,k,\dots) \text{ is odd permutation of } (1,2,3,\dots) \\ 0 & \text{otherwise} \end{cases}$$

→ Cramer's Rule for Inverse

$$M^{-1} = \frac{1}{\det M}[C_{ij}]^T$$

→ Hermitean Conjugation : Complex number matrix

- M^* def. $(M^*)_{ij} = (M_{ij})^*$
- $M^* = M$; M 라고 real
- $(M^*)^T = (M^T)^* := M^\dagger \rightsquigarrow (AB)^\dagger = B^\dagger A^\dagger$
  ↳ "Hermitean conjugate"
- $M^\dagger = M$; M 라고 Hermitean matrix

* $M\vec{x} = \vec{0}$ has a solution $\leftrightarrow$ $\det M = 0$
  (non-trivial $\vec{x} \neq \vec{0}$)

→ Eigenvectors & Eigenvalues

$\vec{y} = M\vec{x}$, eigenvector of M is $\vec{\psi}$ s.t. $M\vec{\psi} = \lambda\vec{\psi}$

(eigenvalue λ is associated with $\vec{\psi}$ and $\lambda \in \mathbb{C}$)

โดยปกติ $\vec{\psi}$ จะ normalize ด้วย.

Solving, $M\vec{\psi} = \lambda\vec{\psi}$

$(M-\lambda I)\vec{\psi} = \vec{0}$

For $\vec{\psi} \neq \vec{0}$, $\det(M-\lambda I) = 0$

โดย $M-\lambda I$: $M_{ii} \mapsto M_{ii} - \lambda$

$\therefore$ $\det(M-\lambda I)$ เป็นพหุนามดีกรี n ($M_{n\times n}$)

e.g. $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \rightarrow M-\lambda I = \begin{pmatrix} a-\lambda & b \\ c & d-\lambda \end{pmatrix}$

$|M-\lambda I| = (a-\lambda)(d-\lambda) - bc$

$|M-\lambda I| = \lambda^2 - (a+d)\lambda + (ad-bc) = 0$

$\therefore \lambda_\pm = \frac{1}{2}\left((a+d) \pm \sqrt{(a-d)^2+4bc}\right)$

→ Let $\vec{\psi} = \begin{pmatrix} x \\ y \end{pmatrix}$, $\begin{pmatrix} a-\lambda & b \\ c & d-\lambda \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = 0$

$\therefore \vec{\psi}_+ = \begin{pmatrix} b \\ \lambda_+ - a \end{pmatrix} = \begin{pmatrix} \lambda_+ - d \\ c \end{pmatrix}$

$\vec{\psi}_- = \begin{pmatrix} b \\ \lambda_- - a \end{pmatrix} = \begin{pmatrix} \lambda_- - d \\ c \end{pmatrix}$

ยาก M เป็น hermitean : $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}$

($M = M^{*T} = M^\dagger$)

จะได้ $a, d \in \mathbb{R}$

$b = c^*$

Case $n \times n$ matrix : $\lambda_a : a \in 1..n$ s.t.

For M an Hermitean ($M = M^\dagger$)

$$M\vec{\psi}_a = \lambda_a \vec{\psi}_a$$

$$\vec{\psi}_a^\dagger M^\dagger = \vec{\psi}_a^\dagger \lambda_a^*$$

$$\vec{\psi}_a^\dagger M^\dagger \vec{\psi}_b = \lambda_a^* \vec{\psi}_a^\dagger \vec{\psi}_b \quad -(1)$$

$$\vec{\psi}_b^\dagger M \vec{\psi}_a = \lambda_a^* \vec{\psi}_b^\dagger \vec{\psi}_a$$

equiv

$$\vec{\psi}_a^\dagger M \vec{\psi}_b = \lambda_b \vec{\psi}_a^\dagger \vec{\psi}_b \quad -(2)$$

$(1)-(2)$: $(\lambda_a^* - \lambda_b)\vec{\psi}_a^\dagger \vec{\psi}_b = 0$ ...

→ Diagonalization

$M_{n\times n}$; $\lambda_a, \vec{\psi}_a$: $a \in 1..n$, $S = (\psi_1, \psi_2, \ldots, \psi_n)$

$$S^{-1} = \begin{pmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{pmatrix} \rightarrow S^{-1}S = I \quad : \phi_a \psi_b = \delta_{ab}$$

⋮

→ Sets are disjoint $\leftrightarrow$ $\forall a \in A, \forall b \in B (a \notin B \wedge b \notin A)$ i.e. $\{1,2\}, \{3,4\}$ are disjoint.

→ Partition of set

e.g. $\{1,2,3\}$ 의 partition 예는 $\{\{1,2\},\{3\}\}$ (cells), $\{\{1\},\{2\},\{3\}\}$, ...

$1\,2 \mid 3$ $\quad$ $1 \mid 2 \mid 3$

Refer to: Fraleigh

① Groups & Subgroups

$S \times S = \{(a,b) : a,b \in S\}$

■ Binary Operation ($*$)

def $f: S \times S \to S \leftrightarrow *(a,b)) \leftrightarrow a * b$

def $H \subseteq S$, subset H is closed under $*$ if $\forall a,b \in H (a*b \in H)$ (by def.)

e.g. $\mathbb{R}$ does NOT induce op. on $\mathbb{R}^*$ (non-zero $\mathbb{R}$) $\because -2 \in \mathbb{R}^* \wedge 2 \in \mathbb{R}^*$ but $(-2)+2 \notin \mathbb{R}^*$

def $*$ on S is commutative $\leftrightarrow$ $a*b = b*a$ for all $a,b \in S$

def $*$ on S is associative $\leftrightarrow$ $(a*b)*c = a*(b*c)$ for all $a,b,c \in S$

$\therefore a*b*c$ is not ambiguous.

Thm Associativity of Composition

$f,g,h : S \to S \longrightarrow f \circ (g \circ h) = (f \circ g) \circ h$

def S with $*$, $\forall a \in S (e \in S \wedge a*e = e*a = a) \to e$ is neutral element (identity element) for $*$.

Thm Uniqueness of Neutral : $\exists! e \in S$; S with $*$

pf. by contradiction, let e, e' be neutrals.

$e * e' = e'$ $\because$ e is a neutral

$e * e' = e$ $\because$ e' is a neutral

$\therefore e = e' \longrightarrow$ There is one neutral. ■

def S with $*, e$: $\forall a \in S\,(x \cdot x^{-1} = x^{-1} \cdot x = e) \rightarrow x^{-1}$ is an inverse of x.
(x^{-1}) (x^{-1}) (x^{-1})

- **Group** — group has at least one element : e — CLOSURE (G_0)

def A group $\langle G, * \rangle$ is a set G closed under bin. op. $*$ s.t.

groupoid
semigroup
monoid
group

$\wedge \begin{cases} G_1 : a,b,c \in G : (a*b)*c = a*(b*c) : \text{associativity of } * \\ G_2 : \text{There exists } e \in G \text{ s.t. } \forall x \in G : e*x = x*e = x : \text{neutral } e \text{ for } * \quad (e: \text{identity}) \\ G_3 : a \in G : a*a' = a'*a = e : \text{inverse } a' \text{ of } a \end{cases}$

def A group G is abelian if $*$ is commutative.

def+ Semigroup is a set with associative bin. op.
def+ Monoid is a semigroup with an identity element.
} Every group is both semigroup and monoid.

def Group G : the order of G is cardinality of G : $|G|$.

⊕ def order of element $a \in G$ = least n s.t. $a^n = 1$ ($|a| = |\langle a \rangle|$)

- **Group Isomorphism**

e.g. G_1:

×	1	−1
1	1	−1
−1	−1	1

G_2:

*	e	a
e	e	a
a	a	e

$a*a' = a'*a = e$
$a' = \cancel{e}$ or a ✓
$\because a*e \neq e$ → $a = e$ ✗
→ $a*a = e$

$\therefore G_1$ and G_2 are not equal but isomorphic

$G_1 : \langle \{-1, 1\}, \times \rangle$, $G_2 : \langle \{e, a\}, * \rangle \rightarrow G_1 \simeq G_2$ ($G_1 \cong G_2$ ก็ได้)

def Let $G_1 : \langle S_1, *_1 \rangle$ and $G_2 : \langle S_2, *_2 \rangle$ be groups and $f : S_1 \rightarrow S_2$.

Then, f is a group isomorphism if

$\wedge \begin{cases} 1.\ f \text{ is bijective } (\underset{\text{onto}}{\text{surjective}} \ \& \ \underset{1\text{-}1}{\text{injective}}). \\ 2.\ \forall a,b \in S_1\,(f(a *_1 b) = f(a) *_2 f(b)). \end{cases}$

↳ called "homomorphism property" : Relabling in 1. makes $*_1, *_2$ matches.

↓ (structure-preserving map)

makes $f^{-1} : S_2 \rightarrow S_1$ ($G_1 \simeq G_2 \leftrightarrow G_2 \simeq G_1$)

(ตัวอย่าง groups) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ under addition.

$GL(n, \mathbb{R})$ "General Linear Group" or $GL_n(\mathbb{R})$ under mat.mul.

↳ The set of $n \times n$ invertible matrices.

แต่ $M_{m \times n}(\mathbb{R})$ ไม่เป็น Group (under mat.mul.)

Group Tables

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

→ ด้วยสมบัติการมี inverse ของ a และ $a \neq b$ และ uniqueness

จะ: ใช้ $a*a' = e$ ใน row XOR column 1 ตัว

ดังนั้น $a*x = e$ และ $y*a = e$ have unique sols.

และ $a*x = b$ และ $y*a = b$ have unique sols.

Abelian Groups Examples

Defining $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, $|\mathbb{Z}_n| = n$ (cardinality)

Defining $+_n$, let $a, b \in \mathbb{Z}_n$,

$$a +_n b = \begin{cases} a+b & a+b < n \\ a+b-n & a+b \geq n \end{cases}.$$

↓ "addition modulo n"

$\therefore$ $a +_n b \in \mathbb{Z}_n$ → closure

$a +_n b = b +_n a$ → commutative

0 is identity

$n-a$ is inverse of a

⊕ Klein four-group (K_4 or V) is the smallest group that is not cyclic. (Abelian group)

– Some complex numbers properties : $|z|$: modulus, $\arg(z)$: argument

$z = a + bi$

$z = |z|(\cos\theta + i\sin\theta)$

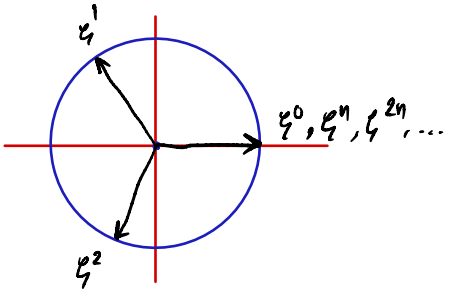
$e^{i\theta} = \cos\theta + i\sin\theta$

$z = |z| e^{i\theta}$

$$z_1 z_2 = |z_1||z_2|\left[\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2)\right]$$

Algebra on Unit Circle

Let $U = \{z \in \mathbb{C} : |z| = 1\}$



Thm $\langle U, \cdot \rangle$ is abelian group.

Roots of Unity : $e^{i(m\frac{2\pi}{n})} = \cos\left(m\frac{2\pi}{n}\right) + i\sin\left(m\frac{2\pi}{n}\right)$; $m = 0..(n-1)$

; $U_n \subseteq U$. Let $\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ (closed under $\cdot$)

n^{th} roots of unity : $1 = \zeta^0, \zeta^1, \zeta^2, \ldots, \zeta^{n-1}, 1 = \zeta^n$

U_n : Points of n-gon's vertices.

■ Non-abelian Groups Examples

NOTATION	$*$	$+$	$\cdot$ (ใช้ Notation นี้)
	Maybe	Abelian	Maybe
	e	0	1
	a'	$-a$	a^{-1}
	$a*b$	$a+b$	ab
	$\underbrace{a*\dots*a}_{k}$	ka	a^k
	$\underbrace{a'*\dots*a'}_{k}$	$-ka$	a^{-k}

def Permutation of set $A \equiv \phi : A \xrightarrow{1\text{-}1,\ \text{onto}} A$

Permutation Groups : function composition $\circ$ is "permutation multiplication."
(collection of all permutations of A)

Let A be set, σ, τ เป็น permutation ของ A,

$\sigma\circ\tau \equiv A \xrightarrow{\sigma} A \xrightarrow{\tau} A \equiv \sigma\tau$; $\sigma\tau$ is also bijective.

e.g. $A = \{1,2,3,4,5\}$

$\sigma = (1,4,3,5)$ – disjoint cycle

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$ หมายถึง $\sigma(1)=4,\ \sigma(2)=2,\dots$

$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} \rightarrow \tau = (1,3,4,2,5)$ | $\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix} = (1,5,2,4,3)$

$\therefore \sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$

ทำ τ ก่อน แล้วทำ σ $\therefore \sigma\tau(1) = \sigma(\tau(1)) = \sigma(3) = 5$

Thm. A is nonempty set. S_A is collection of all permutations of A. Then,
S_A is a group under permutation multiplication.

Properties : CLOSURE ✓

ASSOCIATIVITY ✓

NEUTRAL $\sigma(a) = a$; $a \in A$ ✓

INVERSE $\sigma(a) = b \rightarrow \sigma^{-1}(b) = a$ ∵ 1-1, onto ✓

COMMUTATIVITY ✗ $(\sigma\tau \neq \tau\sigma) \rightarrow$ Non-abelian.

Disjoint Cycles : ภาษาไทย permutation อย่างนี้นะ

Cycle

e.g. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix} = (1,3,6)(2,4)$ หรือ $(1,3,6)(2,4)(5)$ ← More preferred.

↳ product of 3-cycle and 2-cycle

* Order doesn't matter ↳ $= (3,6,1)(2,4) = (2,4)(6,1,3) = \ldots$ but keep cyclicity *

Transposition : 2-cycle (ภาษาไทย 2 element ใน permutation)

def Collection of Cycles is **disjoint** if an element appears only once (one cycle only).

e.g. $(1,3,6)(2,4)$ is disjoint

$(1,3,6)(1,4)$ is not disjoint

def Group of all permutations of $\{1,2,\ldots,n\}$ is **symmetric group on n letters.**

Denoted by S_n, $|S_n| = n!$

* Any $P \in S_n$ can be written in disjoint cycle notation.

Dihedral Group

A collection of finite groups under symmetries of "regular" n-gons.

Note $U_n \simeq \mathbb{Z}_n$, U_n contains vertices. → Denoted by P_n

Note Edges of P_n : line segments between vertices k and $k +_n 1$; $k = 0..(n-1)$ $(k \in \mathbb{Z}_n)$

def Let $n \geq 3$. $D_n \equiv$ set of all $\phi : \mathbb{Z}_n \xrightarrow{1-1} \mathbb{Z}_n$ which → AKA, $S_{\mathbb{Z}_n}$

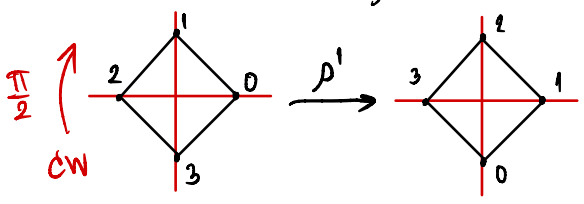
line segment between vertices i, j is an edge of $P_n \leftrightarrow$

line segment between vertices $\phi(i), \phi(j)$ is an edge of P_n

* ϕ is some transformation with some symmetry. → Permutation.

* $\langle D_n, \circ \rangle$ is a group for any $n \geq 3$.

e.g. Let $n \geq 3$. $\rho : \mathbb{Z}_n \to \mathbb{Z}_n$: rotating P_n by $\frac{2\pi}{n}$ CW. ***

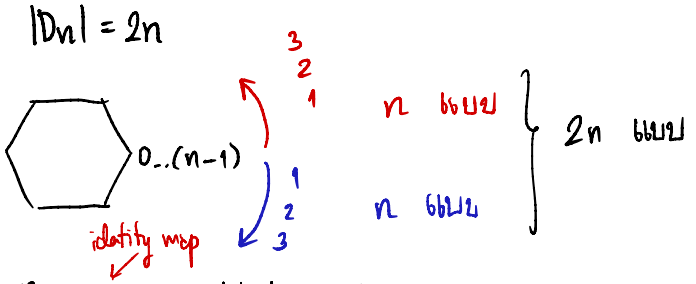


$\therefore$ $\rho(0) = 1$, $\rho(1) = 2$, $\rho(2) = 3$, $\rho(3) = 0$ $\Big\}$ $\rho(k) = k +_n 1$; $k \in \mathbb{Z}_n$

Reflection on X-axis also works : $\mu(k) = -k$

Thm Let $n \geq 3$, $|D_n| = 2n$

Intuitive proof:



Properties

1. $\rho^n = 1$ (Rotate by 2π)
2. $(\rho^k)^{-1} = \rho^{n-k}$
3. $\mu^2 = 1$, $\mu^{-1} = \mu$
4. $\rho^k \mu = \mu \rho^{n-k}$

Subgroups

Subset : $\mathbb{Z} \subseteq \mathbb{Q}$, $\mathbb{Q} \subseteq \mathbb{R}$ ⟶ care about operations : subgroup.

def (Subset H of group G is closed under bin. op. of G

∧ H with induced operation from G is a group.) ⟶ H is a subgroup of G.

Denoted by $H \leq G$ or $G \geq H$.

* $H < G$ means $H \leq G$ but $H \neq G$

$\therefore \langle \mathbb{Z}, + \rangle < \langle \mathbb{R}, + \rangle$ but $\langle \mathbb{Q}^+, \cdot \rangle \not< \langle \mathbb{R}, + \rangle$ even though $\mathbb{Q}^+ \subset \mathbb{R}$

* Every group G has subgroup G itself and $\{e\}$

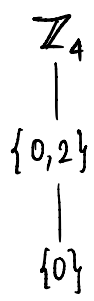
def Let G be a group, $H \leq G$. $H = G$ → H is improper subgroup.

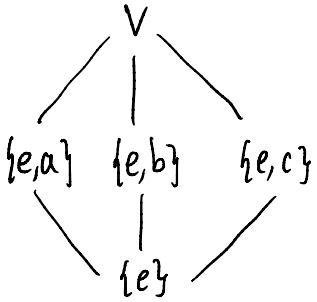
$H \neq G$ → H is proper subgroup.

$\{e\}$ is trivial subgroup;

else, nontrivial subgroup.

Subgroup diagram





Thm Subset H of group G is subgroup of G $\leftrightarrow$

1. H is closed under bin. op. of G
2. Neutral e of G is in H
3. $\forall a \in H : a^{-1} \in H$

Cyclic Subgroups

e.g. $\mathbb{Z}_{12} \geq H$; $H = \{0, 3, 6, 9\}$ which H is cyclic.

Thm Let G be group and $a \in G$.

$H = \{a^n : n \in \mathbb{Z}\}$ is a subgroup of G and is the smallest subgroup of G containing a.

* Every subgroup containing a will contain H.

Pf. 1. $a^r a^s = a^{r+s}$; $r, s \in \mathbb{Z}$ $\rightarrow$ closed in H.

2. $a^0 = e$ $\rightarrow$ neutral.

3. $a \in H$, $a^{-1} \in H$, $aa^{-1} = e$ $\rightarrow$ inverse. ■

def Let G be a group, $a \in G$.

Subgroup $\{a^n : n \in \mathbb{Z}\}$ of G is a cyclic subgroup generated by a.

Denoted: $\langle a \rangle$

e.g. (Review: Dihedral Group)

$(\mu\rho^k)^2 = \mu\rho^k\mu\rho^k = \rho^{n-k}\mu^2\rho^k = \rho^n = 1$

$(\mu\rho^k)^{-1} = \rho^{n-k}\mu^{-1}\mu$

$(\mu\rho^k)^{-1} = \mu\rho^k$

* Inverse: $(a^2b^4a^{-3}b^6a^5)^{-1} = a^{-5}b^{-2}a^3b^{-4}a^{-2}$

D_{10} : $\langle \mu\rho^k \rangle$; $k \in \mathbb{Z}_{10} \rightarrow (\mu\rho^k)^r = 1$ or $\mu\rho^k$

$\therefore \langle \mu\rho^k \rangle = \{1, \mu\rho^k\}$.

def An element $a \in G$ generates G and is a generator for G if $\langle a \rangle = G$.

* Group G is cyclic if $\exists a \in G$ generates G. *

e.g. $\mathbb{Z}_4$ is cyclic. 1, 3 are generators: $\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$

Cyclic Groups

เกริ่น Let G be group, $a \in G$.

$\langle a \rangle \leq G$ and $\langle a \rangle$ is finite $\rightarrow$ $|\langle a \rangle|$ is order of subgroup $\langle a \rangle$.

Otherwise, $\langle a \rangle$ has infinite order. ($|a| \equiv |\langle a \rangle|$)

Properties (CYCLIC GROUPS)

Thm Every cyclic group is abelian.

Pf. Let G be cyclic group. a is generator of G: $G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}$

$g_1, g_2 \in G : \exists r,s \in \mathbb{Z}$ s.t. $g_1 = a^r$ and $g_2 = a^s$

Then, $g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1$.

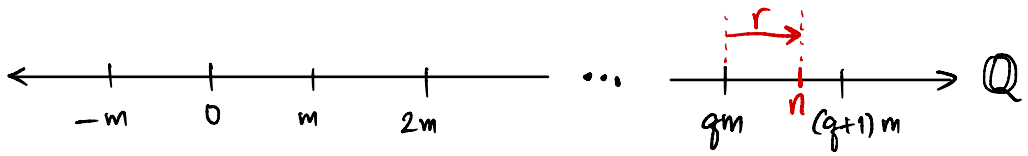
$\therefore$ G is abelian. ■

Division Algorithm ($\mathbb{Z}$)

$n \div m$ yields quotient q and remainder r: $n \div m = q \; R \; r$:

$\frac{n}{m} = q + \frac{r}{m} \rightarrow n = qm + r \quad (0 \leq r < m)$

Diagram Pf



n falls on multiple of m if $r=0$ or n falls between two multiples of m if $r \neq 0$

① $r=0$ ② $r>0$

If ②, let qm be the first multiple of m that is to the left of n $(qm < n)$

$\therefore$ $0 \leq r < m$. Uniqueness : when n is not a multiple of m, take $r=0$, then there is a unique multiple of m : qm to the left of n at distance always less than m. ■

Thm. A subgroup of a cyclic group is cyclic.

Pf. Let G be a group generated by a. $H \leq G$.

If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic.

If $H \neq \{e\}$, then $a^n \in H$ $(\exists n \in \mathbb{Z}^+)$. Let m be the smallest integer in $\mathbb{Z}^+$ s.t. $a^m \in H$.

Claim: $c = a^m$ generates H; $H = \langle c \rangle = \langle a^m \rangle$

Show that every $b \in H$ is a power of c. Since $b \in H$, $H \leq G$: $b = a^n$ (for some n) Find q, r s.t. $n = mq + r$; $0 \leq r < m$

Using div. algo.: $a^n = a^{mq+r} = (a^m)^q a^r$

$\therefore a^r = (a^m)^{-q} a^n$

We supposed $a^n, a^m \in H$. $\therefore (a^m)^{-q} \in H \rightarrow (a^m)^{-q} a^n \in H$.

$\therefore a^r \in H$.

m smallest $\wedge$ $a^m \in H$ $\wedge$ $0 \leq r < m \rightarrow r = 0$. We get $n = mq$.

$b = a^n = (a^m)^q = c^q$. ■

(+) **def** Let $r \in \mathbb{Z}^+$, $s \in \mathbb{Z}^+ \cup \{0\}$.

Generator d of the cyclic group $H = \{nr + ms : n, m \in \mathbb{Z}\}$ under addition op. is gcd of r, s. $d = \gcd(r, s) = nr + ms$ Bézout's Identity

Cyclic Groups' Structures

Thm Let G be cyclic group with gen. a. If $\text{ord}(G)$ is infinite, then $G \simeq \langle \mathbb{Z}, + \rangle$

If $\text{ord}(G) = |G| = n$, then $G \simeq \langle \mathbb{Z}_n, +_n \rangle$

Subgroups of Finite Cyclic Groups

Thm Let $G = C_n = \langle a \rangle$. Let $b \in G$, $b = a^s$.

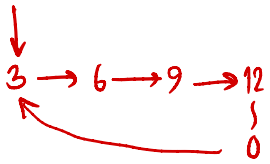
Then $H \leq G : H = \langle b \rangle$, $|H| = n/d$; $d = \gcd(n, s)$.

$* \ \langle a^s \rangle = \langle a^t \rangle \leftrightarrow \gcd(s, n) = \gcd(t, n)$.

e.g. Consider $\mathbb{Z}_{12}$ with $\langle a \rangle$; $a = 1$.

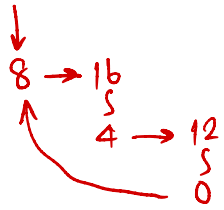
- $\gcd(12, 3) = 3$

  $|H| = \frac{12}{3} = 4 \rightarrow \langle 3 \rangle = \{0, 3, 6, 9\}$.



- $\gcd(12, 8) = 4$

  $|H| = \frac{12}{4} = 3 \rightarrow \langle 8 \rangle = \{0, 4, 8\}$.



- $\gcd(12, 5) = 1$

  $|H| = \frac{12}{1} = 12 \rightarrow \langle 5 \rangle = \mathbb{Z}_{12}$.

Col $\gcd(n, s) = 1 \rightarrow \langle s \rangle = C_n$

Col Let G be finite cyclic group. $H \leq G \rightarrow |H| \mid |G|$. ($|G|$ is a multiple of $|H|$)

↳ Lagrange's Thm ใช้กับกลุ่มที่ไม่ cyclic!

⊕ Orders of subgroups of C_n are all $a : a \mid n$

eg. $\mathbb{Z}_{28}$: $28 = 2^2 \cdot 7$

∴ Orders of subgroups of $\mathbb{Z}_{28}$ are $1, 2, 4, 7, 14, 28$

$|\langle 0 \rangle| = 1$, $|\langle 14 \rangle| = 2$, $|\langle 7 \rangle| = 4$, $|\langle 4 \rangle| = 7$, ...

Generating Sets & Cayley Digraphs

Prod. Integral powers : $a^n b^n \ldots$

Products of Integral Powers of a, b form subgroup of G :

a, b are <u>generators</u>. $\{a, b\}$ <u>generates</u> G if the subgroup is all of G.

<u>e.g.</u> $\{\mu, \rho\}$ generates D_n for $a \in D_n$, $a = \rho^k$ or $\mu\rho^k$; $k \in \mathbb{Z}_n$

<u>e.g.</u> $\mathbb{Z}_6$ is generated by $\{1\}$, $\{5\}$. Also, by $\{2, 3\}$ $\because 2+3=5$

Also, $\{3,4\}$, $\{2,3,4\}$, $\{1,3\}$, $\{3,5\}$ but not $\{2,4\}$ $\because \langle 2 \rangle = \{0,2,4\}$

<u>def</u> Let $\{S_i : i \in I\}$. I is any indices.

$\bigcap_{i \in I} S_i$ (Intersection) of sets S_i is "set of all elements that are in all sets S_i.

$\rightarrow$ $\bigcap_{i \in I} S_i = \{x : \forall i \in I (x \in S_i)\}$

For finite $I = \{1, 2, \ldots, n\}$: $\bigcap_{i \in I} S_i = S_1 \cap S_2 \cap \ldots \cap S_n$

<u>Thm</u> Any group G and any nonempty $\{H \leq G : i \in I\}$, $\bigcap_{i \in I} H_i \leq G$.

<u>def</u> Let G be group, $a_i \in G$; $i \in I$.

The smallest subgroup containing $\{a_i : i \in I\}$ is the subgroup gen. by $\{a_i : i \in I\}$.

If subgroup $= G$, $\{a_i : i \in I\}$ <u>generates</u> G and a_i are <u>generators</u>.

If there is finite $\{a_i : i \in I\}$ generating G, G is <u>finitely generated</u>.

<u>Thm</u> Let G be group,

$a_i \in G$; $i \in I \neq \emptyset$ $\rightarrow$ $H \leq G$ gen. by $\{a_i : i \in I\}$ has elements of G that...

are finite prod. of integral powers of a_i

<u>e.g.</u> $D_n \equiv S_{\mathbb{Z}_n}$ (edges in P_n).

$\rho = (0, 1, 2, \ldots, n-1)$

$\mu = (1, n-1)(2, n-2)\ldots\left(\frac{n-1}{2}, \frac{n+1}{2}\right)$; $2 \nmid n$

or $\left(\frac{n-2}{2}, \frac{n+2}{2}\right)$; $2 \mid n$

and $\rho^n = 2$, $\mu^2 = 2$: μ^0, μ^1 ; $\rho^0, \rho^1, \ldots, \rho^{n-1}$ $\rightarrow$ comb.

μ, ρ are generators : $S_{\mathbb{Z}_n} = \{2, \rho, \rho^2, \ldots, \rho^{n-1}, \mu, \mu\rho, \ldots, \mu\rho^{n-1}\}$

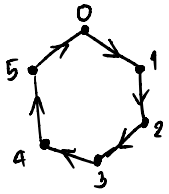
$= D_n$ □

Cayley Digraphs (Directed Graph)

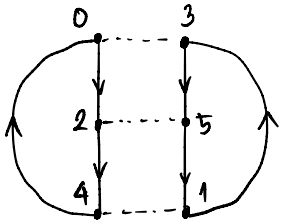
$x \xrightarrow{a} y \equiv xa = y \;,\; ya^{-1} = x$

$x \overset{b}{\cdots} y \equiv b^2 = e$ (b is its own inverse) $\equiv x \rightleftarrows y$

eg. $\mathbb{Z}_6$ with generating set $S = \{1\}$ ($\xrightarrow{1}$)



eg. $\mathbb{Z}_6$ with $S = \{2, 3\}$ ($\xrightarrow{2}$, $\overset{3}{\cdots}$) → 3 is its own inverse. $3 +_6 3 = 0$



---

② Structure of Groups

Groups of Permutations

Let $\phi : G \to G'$. $\phi(ab) = \phi(a)\phi(b)$. ϕ is a group homomorphism.

* Any group isomorphism is group homomorphism. (iso = homo + bij.)

eg. $\phi : \mathbb{R} \to U$ (Unity) : $\phi(x) = \cos(2\pi x) + i\sin(2\pi x) = e^{2\pi i x}$

For $a, b \in \mathbb{R}$: $\phi(a+b) = e^{2\pi i(a+b)} = e^{2\pi i a} e^{2\pi i b} = \phi(a)\phi(b)$.

ϕ maps $\mathbb{R}$ onto U but not 1-1.

def Let $\phi : X \to Y$, suppose $A \subseteq X$ and $B \subseteq Y$.

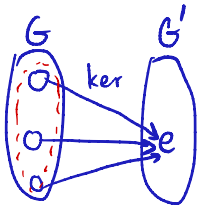
$\phi[A] = \{\phi(a) : a \in A\} \equiv$ image of A in Y under mapping ϕ.

$\phi^{-1}[B] = \{a \in A : \phi(a) \in B\} \equiv$ inverse image (preimage) of B in X under mapping ϕ.

Thm Let ϕ be homomorphism of G into G'.

1. identity $e \in G \to$ identity $e' = \phi(e) \in G'$
2. $a \in G \to \phi(a^{-1}) = \phi(a)^{-1}$
3. $H \leq G \to \phi[H] \leq G'$
4. $K' \leq G' \to \phi^{-1}[K'] \leq G$

} ϕ preserves identity, inverses, subgroups.



def Let $\phi : G \to G'$ $\quad \ker(\phi)$ = preimage of ϕ that maps to e (e') of G'

Subgroup $\phi^{-1}[\{e'\}] = \{x \in G : \phi(x) = e'\} = \ker(\phi)$ "kernel of ϕ".

Cayley's Theorem

def Let G be group, λ_x be permutation of elements of G by row x in G table.

$\phi : G \to S_G : \phi(x) = \lambda_x$; $\lambda_x(g) = xg$ for all $g \in G$.

This is called left regular representation of G.

★ **Thm** (Cayley's Thm.) Every group is isomorphic to a group of permutation.

Pf. Let G be group. $\phi : G \to S_G : \phi(x) = \lambda_x$.

Must verify ϕ : homomorphism & 1-1.

By thm., $\phi[G] \leq S_G$ and $\phi : G \to \phi[G]$ is isomorphism.

$a, b \in G$, $\phi(a) = \phi(b) \to \lambda_a = \lambda_b \to \lambda_a(e) = \lambda_b(e) \to ae = be \to a = b$.

$\phi(ab) = \lambda_{ab}$, $\phi(a)\phi(b) = \lambda_a \lambda_b$: □

$\lambda_{ab}(g) = (ab)g = a(bg) = \lambda_a(bg) = \lambda_a(\lambda_b(g)) = (\lambda_a \lambda_b)(g)$.

$\therefore \lambda_{ab} = \lambda_a \lambda_b$ ■

def+ Let G be group, σ_x be permutation of elements of G by col. x in G table.

$\tau : G \to S_G : \tau(x) = \sigma_{x^{-1}}$; $\sigma_x(g) = gx$ for all $g \in G$.

This is called right regular representation of G.

Permutations

def A cycle of length 2 is a transposition.

* $(a_1, a_2, \dots, a_n) = (a_1, a_n)(a_1, a_{n-1})\dots(a_1, a_3)(a_1, a_2)$.

n-cycle; $n-1$ transpositions.

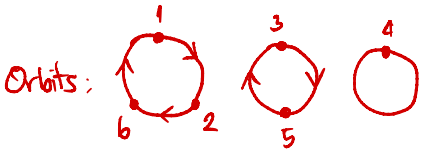
Thm Any permutation of a finite set with $|S| \geq 2$ is a product of transpositions. (by def.)

e.g. $(1,6)(2,5,3) = (1,6)(2,3)(2,5)$

Orbit: Let $\sigma \in S_A$, $a \in A$. $\mathrm{Orb}(a) = \{\sigma^k(a) : k \in \mathbb{Z}\}$

Case $\sigma \in S_n$: $\mathrm{Orb}(a)$ = elements containing a in disjoint cycle repr. of σ.

e.g. $\sigma = (1,2,6)(3,5) \in S_6$. $\mathrm{Orb}(1) = \mathrm{Orb}(2) = \mathrm{Orb}(6) = \{1,2,6\}$



$\mathrm{Orb}(3) = \mathrm{Orb}(5) = \{3,5\}$

$\mathrm{Orb}(4) = 4$ ($\sigma = (1,2,6)(3,5)(4)$).

Thm Permutation in S_n can be expressed either as even # transpositions or as odd # transpositions, not both. (proof, Fraleigh, 83)

def A permutation of a finite set is even or odd according to # transpositions.

e.g. Identity permutation in S_n is even.

$(1,4,5,6)(2,1,5) = (1,6)(1,5)(1,4)(2,5)(2,1)$ is odd permu.

Alternating Groups

Claim: For $n \geq 2$, #even permu. S_n = #odd permu. S_n = $\frac{n!}{2}$

Pf: A_n = {even permu.}, B_n = {odd permu.} → define $f : A_n \to B_n$ (1-1, onto) shows $|A_n| = |B_n|$.

Let $\tau = (1,2)$ for $n \geq 2$, $\lambda_\tau : A_n \to B_n$: $\lambda_\tau(\sigma) = \tau\sigma$.

which $\sigma \in A_n \xrightarrow{\lambda_\tau} (1,2)\sigma$ ... (proof, Fraleigh, 84)

Thm $n \geq 2 \rightarrow |\{\text{even perm. of } S_n\}| = \frac{n!}{2}$

Sign of permutation: $\operatorname{sgn} : S_n \to \{-1, 1\}$: $\operatorname{sgn}(\sigma) = \begin{cases} 1 & \sigma \text{ is even;} \\ -1 & \sigma \text{ is odd.} \end{cases}$

def Subgroup of S_n consisting of even permutations of n letters is **alternating group** on n letters A_n.

Finitely-Generated Abelian Groups

def Cartesian Product of sets : $\prod_{i=1}^{n} B_n = B_1 \times B_2 \times \dots \times B_n$

Thm Let $G_1, G_2, \dots, G_n$ be groups.

For $(a_1, a_2, \dots, a_n), (b_1, b_2, \dots, b_n) \in \prod^{n} G_i$, under bin. op.

Direct product of groups $G_i = \prod_{i=1}^{n} G_i = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$ which is a group.

i.e., G with $*$, H with Δ: $G \times H = \langle S, \bullet \rangle$;

$S = \{(g, h) : g \in G, h \in H\}$

$\bullet : (g_1, h_1)(g_2, h_2) = (g_1 * g_2, h_1 \Delta h_2)$.

having Closure, Associativity, Neutral, Inverse.

If operations in G_i is commutative, i.e., abelian,

Direct sum of groups $G_i = \bigoplus_{i=1}^{n} G_i = G_1 \oplus G_2 \oplus \dots \oplus G_n$ is used.

e.g. $\mathbb{Z}_2 \times \mathbb{Z}_3$; $|\mathbb{Z}_2 \times \mathbb{Z}_3| = 2 \times 3 = 6$. ; operations are $(+_2, +_3)$

↳ $(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)$

Try: $(1,1)$:

$$\begin{aligned} (1,1) &= (1,1) \\ 2(1,1) &= (1,1)+(1,1) = (0,2) \\ 3(1,1) &= 2(1,1)+(1,1) = (1,0) \\ 4(1,1) &= (0,1) \\ 5(1,1) &= (1,2) \\ 6(1,1) &= (0,0). \end{aligned}$$

$\therefore$ $(1,1)$ is a generator of $\mathbb{Z}_2 \times \mathbb{Z}_3$ which is cyclic.

$\therefore$ Also, $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$.

Thm $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic and isomorphic to $\mathbb{Z}_{mn} \leftrightarrow \gcd(m,n) = 1$.

($\gcd(m,n) \neq 1$: จะมีอย่างน้อย summand ที่ order หาร mn ลงตัว ไม่ isomorphic กับ $\mathbb{Z}_{mn}$
$\because |\mathbb{Z}_m \times \mathbb{Z}_n| \neq |\mathbb{Z}_{mn}|$)

Col+ $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ is cyclic and isomorphic to $\mathbb{Z}_{m_1 m_2 \cdots m_n} \leftrightarrow$ All $\gcd(m_i, m_j) = 1$

e.g. $m_i \in \{\text{Primes}\}$, $m_i \in \{8, 9\}$

$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \simeq \mathbb{Z}_{42}$ $\quad$ $\mathbb{Z}_8 \times \mathbb{Z}_9 \simeq \mathbb{Z}_{72}$

Thm Let $(a_1, a_2, \ldots, a_n) \in \prod_{i=1}^{n} G_i$. a_i is of $r_i \in G_i \rightarrow (a_1, a_2, \ldots, a_n)$'s order $= \text{lcm}(r_i)$

e.g. Find the order of $(8,4,10)$ in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.

$\gcd(12,8) = 4 \rightarrow \frac{12}{4} = 3$: 8's order in $\mathbb{Z}_{12}$ $= 3$

$\gcd(60,4) = 4 \rightarrow \frac{60}{4} = 15$: 4's order in $\mathbb{Z}_{60}$ $= 15$

$\gcd(24,10) = 2 \rightarrow \frac{24}{2} = 12$: 10's order in $\mathbb{Z}_{24}$ $= 12$

$\text{lcm}(3, 15, 12) = 60$

$\therefore (8,4,10)$ is of order 60 in $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$. □

Thm (Variant) Every finitely-generated abelian group G is isomorphic to direct product of cyclic groups:

$$\mathbb{Z}_{(p_1^{r_1})} \times \mathbb{Z}_{(p_2^{r_2})} \times \cdots \times \mathbb{Z}_{(p_n^{r_n})} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z};$$

p_i = primes (may not be distinct) , $r_i \in \mathbb{Z}_{>0}$

e.g. Find all abelian groups, up to isomorphism, of order 360.

$360 = 2^3 \times 3^2 \times 5$:

1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
2. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
3. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
4. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
5. $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
6. $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

Thm (Invariant) Like above, but in form of: (Every finitely gen. abelian group $\simeq$)

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \mathbb{Z}_{d_3} \times \dots \times \mathbb{Z}_{d_k} \times \mathbb{Z} \times \mathbb{Z} \times \dots \times \mathbb{Z};$$

$d_i \geq 2$ and $d_i \mid d_{i+1}$; $1 \leq i \leq k-1$

d_i are <u>invariant factors</u> / <u>torsion coefficients</u>.

e.g. $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_7$

Primes : 2, 3, 7

→ 2	8	4	2	2
→ 3	9	3	1	1
→ 7	7	1	1	1
	↓	↓	↓	↓
	d_4	d_3	d_2	d_1

→ $d_4 = 8 \times 9 \times 7 = 504$
$d_3 = 4 \times 3 \times 1 = 12$
$d_2 = 2 \times 1 \times 1 = 2$
$d_1 = 2 \times 1 \times 1 = 2$

$\therefore G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12} \times \mathbb{Z}_{504}$.

(Applications)

def A group G is <u>decomposable</u> if isomorphic to direct product of 2 proper nontrivial subgroups.

Thm Finite indecomposable abelian groups are exactly cyclic groups C ; $|C|$ = prime

Thm Let G be finite abelian group. $m \mid |G| \rightarrow H \leq G \wedge |H| = m$

Thm $n^2 \nmid m$; $n \geq 2$ → every abelian group order m is cyclic.

Cosets & Lagrange's Theorem

Partitioning G into r cells ; $H \leq G$: $r|H| = |G|$

Cells are cosets of H.

$H \leq G$. partitioning G def. "$\sim_L$ on G." ← equivalence relation (equivalence class).

Thm Let $H \leq G$. $\sim_L$ on G : $a \sim_L b \leftrightarrow a^{-1}b \in H$.

def Let $H \leq G$. Subset $aH = \{ah : h \in H\}$ of G is left coset of H containing a. for $a \in G$.

e.g. Exhibit left coset of subgroup $3\mathbb{Z} \leq \mathbb{Z}$. (additive)

$m + 3\mathbb{Z}$: $m=0$: $3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\}$ $\quad 0 \sim 1$

$m=1$: $1+3\mathbb{Z} = \{\dots, -5, -2, 1, 4, 7, \dots\}$

$m=2$: $2+3\mathbb{Z} = \{\dots, -4, -1, 2, 5, 8, \dots\}$

Thm Let $H \leq G$. $\forall a \in G$: $|aH| = |H|$.

★ **Thm** (Lagrange's Theorem) Let $H \leq G$. $|G|$ is finite. $|H| \mid |G|$.

Pf. Let $n = |G|$, $m = |H|$.

$\forall a \in G$: $|aH| = |H| = m$.

Let r = #cells in partition of G into aH.

$\therefore rm = n \rightarrow m \mid n \rightarrow |H| \mid |G|$. ■

Col Every group of prime order is cyclic.

Thm Let $a \in G$. $|a| \mid |G|$

def Let $H \leq G$. $\#aH \equiv$ index $(G:H)$ of H in G.

* $(G:H)$ may be finite or infinite. If G is finite, $(G:H) = \frac{|G|}{|H|}$.

Thm $H \leq G \wedge K \leq G$ s.t. $K \leq H \leq G$. Suppose $(H:K), (G:H)$ are finite.

Then, $(G:K) = (G:H)(H:K)$.

def (Right cosets) : $a \sim_R b \iff ab^{-1} \in H \leq G$.

$$Ha = \{ha : h \in H\}. \quad \text{for } a \in G.$$

* In abelian group, $a \sim_R b = a \sim_L b = a \sim b$.

Thm Let $\phi : G \to G'$ (Homomorphism). left & right cosets of $\ker(\phi)$ are identical.

* $a, b \in G$ are in the same coset of $\ker(\phi) \iff \phi(a) = \phi(b)$

e.g. Determinant $\det : GL(2, \mathbb{R}) \to \mathbb{R}^*$ (homomorphism).

($e' = 1$, $e = I_2$)

$\ker(\det) = \{ m \in GL(2, \mathbb{R}) \text{ that maps to } 1 \}$

Let $A = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 2 \\ 2 & 2 \end{pmatrix}$: $\det A = \det B = 2$. $\to$ A, B in same cosets of $\ker(\det)$.

Col $\phi : G \to G'$ is 1-1 $\iff$ $\ker(\phi) = \{e\}$; $e \in G$ (= trivial group).

Plane Isometries

Consider Euclidean plane $\mathbb{R}^2$.

Isometry of $\mathbb{R}^2$ is permu. $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ which $\text{dist}(P, Q) = \text{dist}(\phi(P), \phi(Q))$ $\forall P, Q \in \mathbb{R}^2$.

If ψ is isometry of $\mathbb{R}^2$, then $\text{dist}(\psi(\phi(P)), \psi(\phi(Q))) = \text{dist}(\phi(P), \phi(Q)) = \text{dist}(P, Q)$

$\therefore$ Isometries of $\mathbb{R}^2 \leq S_{\mathbb{R}^2}$

* Every isometry is one of 4 types :

1. Translation τ with vector $\vec{v}$
2. Rotation ρ with angle θ
3. Reflection μ with line L
4. Glide reflection γ : product of translation & reflection.

Thm Every finite group G of isometries of the plane is isomorphic to V, $\mathbb{Z}_{n \geq 1}$, or $D_{n \geq 3}$

③ Homomorphisms & Factor Groups

def $\phi : G \to G'$ is a homomorphism if $\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in G$.

* For any groups G, G' there exists at least one homomorphism: trivial homomorphism

$$\phi : G \to G' : \phi(g) = e'$$

Evaluation Homomorphism $\phi_c(f) = f(c)$

↳ $\phi_c(f+g) = (f+g)(c) = f(c) + g(c) = \phi_c(f) + \phi_c(g)$.

Projection Map (π_i)

Let $G = G_1 \times G_2 \times \dots \times G_n$. $\pi_i : G \to G_i : \pi_i(g_1, g_2, \dots, g_n) = g_i$

Factor Groups (Quotient Groups)

Review: cosets table $\mathbb{Z}_6$

$+_6$	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	0	4	1
5	5	2	0	3	1	4

$\oplus$ $(aH)(bH) = (ab)H$

e.g. $5\mathbb{Z} \leq \mathbb{Z}$:

$5\mathbb{Z} = \{\dots, -10, -5, 0, 5, 10, \dots\}$
$1+5\mathbb{Z} = \{\dots, -9, -4, 1, 6, 11, \dots\}$
$2+5\mathbb{Z} = \{\dots, -8, -3, 2, 7, 12, \dots\}$
$3+5\mathbb{Z} = \{\dots, -7, -2, 3, 8, 13, \dots\}$
$4+5\mathbb{Z} = \{\dots, -6, -3, 4, 9, 14, \dots\}$

Let a_1, a_2 be in same cosets of $5\mathbb{Z}$. $\therefore a_2 = a_1 + 5r$; $\exists r \in \mathbb{Z}$.

b_1, b_2 ⟶ . $\therefore b_2 = b_1 + 5s$; $\exists s \in \mathbb{Z}$.

$a_2 + b_2$: $a_2 + b_2 = (a_1 + 5r) + (b_1 + 5s)$

$= (a_1 + b_1) + 5(r+s) \in (a_1 + b_1) + 5\mathbb{Z}$

$\therefore a_2 + b_2$ is in same coset as $a_1 + b_1$.

def Let $H \leq G$. H is a normal subgroup of G ($H \trianglelefteq G$) if $\forall g \in G : gH = Hg$.

* $\ker(\phi)$; ϕ is homomorphism, is a normal subgroup.

e.g. $H \leq G \wedge G$ is abelian $\rightarrow H \trianglelefteq G$.

e.g. Let $H = \{A \in GL(n, \mathbb{R}) : \det A = 1\}$; $\det : GL(n, \mathbb{R}) \rightarrow \mathbb{R}^*$: homo.

$\therefore H = \ker(\det) \rightarrow H \trianglelefteq GL(n, \mathbb{R})$

$H \equiv$ special linear group $\equiv SL(n, \mathbb{R})$

Thm $H \leq G$, $(aH)(bH) = (ab)H \longleftrightarrow H \trianglelefteq G$.

Col $H \trianglelefteq G \rightarrow$ cosets of H form a group G/H under $(aH)(bH) = (ab)H$

def G/H is factor group (quotient group)

e.g. $\mathbb{Z}$ is abelian $\rightarrow$ $n\mathbb{Z} \trianglelefteq \mathbb{Z}$.

Div. Algo.: $m = nq + r$; $0 \le r < n \rightarrow m \in r + n\mathbb{Z}$

$\rightarrow \mathbb{Z}/n\mathbb{Z} = \{k + n\mathbb{Z} : 0 \le k < n\} = \langle 1 + n\mathbb{Z} \rangle$

$\therefore \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ and is cyclic.

Thm Let $H \trianglelefteq G$. $\gamma : G \rightarrow G/H$: $\gamma(x) = xH$: homomorphism with kernel H. ($H = \ker(\phi)$).

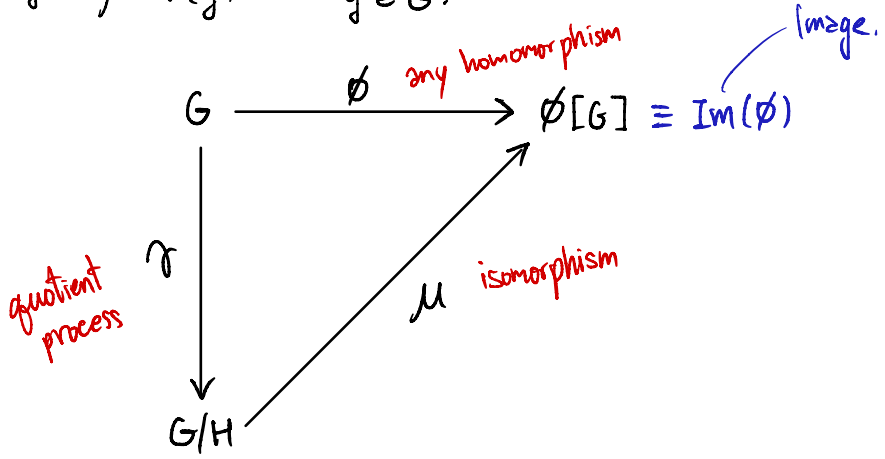
Thm (The Fundamental Homomorphism Thm.)

If: Homomorphism $\phi : G \rightarrow G'$ with $H = \ker(\phi)$.

$\rightarrow \phi[G]$ is a group. $\wedge$ $\mu : G/H \rightarrow \phi[G] : \mu(gH) = \phi(g)$ is isomorphism.

If: Homomorphism $\gamma : G \rightarrow G/H : \gamma(g) = gH$

$\rightarrow \phi(g) = \mu \circ \gamma(g)$ for $g \in G$.



e.g. Classify $(\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2)$

$\pi_1 : \mathbb{Z}_4 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_4$: $\pi_1(x, y) = x$ is homomorphism with $\ker(\pi_1) = \{0\} \times \mathbb{Z}_2$

$\therefore (\mathbb{Z}_4 \times \mathbb{Z}_2)/(\{0\} \times \mathbb{Z}_2) \simeq \mathbb{Z}_4$.

Normal subgroups & inner automorphism

$H \leq G$ s.t. $ghg^{-1} \in H \ \forall g \in G \ \forall h \in H$. $gHg^{-1} = \{ghg^{-1} : h \in H\} \subseteq H \ \forall g \in G$.

Claim: $gHg^{-1} = H$.

Thm Four equivalent conditions for $H \leq G$ to be $H \trianglelefteq G$.

1. $ghg^{-1} \in H \ \forall g \in G \ \forall h \in H$.
2. $gHg^{-1} = H \ \forall g \in G$.
3. There exists homomorphism $\phi : G \to G'$ s.t. $\ker(\phi) = H$.
4. $gH = Hg \ \forall g \in G$.

def Isomorphism $\phi : G \to G$ of group G with itself is an <u>automorphism</u> of G.

$i_g : G \to G : i_g(x) = gxg^{-1} \ \forall x \in G$ is <u>inner automorphism</u>.

↳ "<u>conjugation</u> of x by g".

* $K \leq G$ is a <u>conjugate subgroup</u> of H if $K = i_g[H] = gHg^{-1} \ \exists g \in G$.

$(gH_1g^{-1} = H_2)$

Thm Let $G = H \times K$. $\bar{H} = \{(h,e) : h \in H\}$. $\bar{H} \trianglelefteq G$. $G/\bar{H} \simeq K$. $G/\bar{K} \simeq H$

e.g. $(\mathbb{Z}_4 \times \mathbb{Z}_6)/\langle (0,1) \rangle$

Let $H = \langle (0,1) \rangle = \{(0,0),(0,1),(0,2),(0,3),(0,4),(0,5)\}$.

$|\mathbb{Z}_4 \times \mathbb{Z}_6| = 24$, $|H| = 6 \to |(\mathbb{Z}_4 \times \mathbb{Z}_6)/H| = \frac{24}{6} = 4$.

$\mathbb{Z}_4 \times \mathbb{Z}_6$ is abelian. $\to$ $(\mathbb{Z}_4 \times \mathbb{Z}_6)/H$ is abelian.

$= \{(0,0)+H, (1,0)+H, (2,0)+H, (3,0)+H\}$

$\simeq \mathbb{Z}_4$

Thm G is cyclic $\wedge$ $N \leq G \to G/N$ is cyclic.

Simple Groups

(clearly!)
$\neq \{e\}$ $\neq G$

From Lagrange's, Group with prime order can't have nontrivial proper subgroup.

group ที่มี subgroup ที่ไม่ใช่ $\{e\}$ และตัวมันเอง มีแค่อันเดียว ~ prime number.

def A group is simple if it is nontrivial ∧ has no nontrivial proper normal subgroup.

Thm A_n is simple for $n \geq 5$.

Thm Let homomorphism $\phi : G \to G'$. $N \trianglelefteq G \to \phi[N] \trianglelefteq \phi[G]$.

$N' \trianglelefteq \phi[G] \to \phi^{-1}[N'] \trianglelefteq G$.

"homomorphism $\phi : G \to G'$ preserves normal subgroups between G and $\phi[G]$."

!* Even though $N \trianglelefteq G$, N อาจไม่ normal ใน G'.

def A maximal normal subgroup of a group G is a normal subgroup $M \neq G$ s.t. there is no proper normal subgroup $N < G$ properly containing M.

" $M \trianglelefteq G$ โดยไม่มี $N \trianglelefteq G$ ที่ $M \trianglelefteq N$."

Thm M is maximal normal subgroup of $G \iff G/M$ is simple.

Center & Commutator Subgroups

def center $Z(G)$:

$$Z(G) = \{z \in G : zg = gz \ \forall g \in G\}$$

* $Z(G) \trianglelefteq G$.
* If $Z(G)$ is abelian, $Z(G) = G$.

Requiring $ab = ba$ (abelian), $aba^{-1}b^{-1} = e$ = commutator of a group.

Thm Let G be group. $\{aba^{-1}b^{-1} : a, b \in G\}$ generates C (commutator subgroup) $\trianglelefteq G$.

* If $N \trianglelefteq G$, G/N is abelian $\leftrightarrow C \leq N$

e.g. For S_3, $\rho_0 = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix} = ()$ $(= \rho^0)$ → even permu.

$\rho^1 = \rho_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = (1,2,3)$

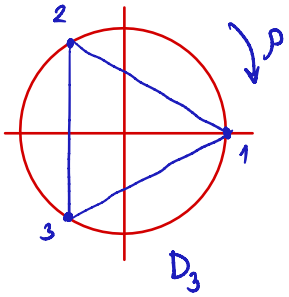
$\rho^2 = \rho_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} = (1,3,2)$

A_3

$\mu_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} = (2,3)$ $(= \mu)$ → odd permu.

$\mu_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = (1,3)$ $(= \mu^1)$

$\mu_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (1,2)$ $(= \mu^2)$



$*$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

S_3

Commutator : $\rho_1\mu_1\rho_1^{-1}\mu_1^{-1} = \rho_1\mu_1\rho_2\mu_1$

$= \mu_3\mu_2 = \rho_2$.

$\rho_2\mu_1\rho_2^{-1}\mu_1^{-1} = \rho_1$.

$\therefore$ C of S_3 contains $A_3 = \{\rho_0, \rho_1, \rho_2\}$

Since $A_3 \trianglelefteq S_3$ e.g. ghg^{-1}: $\rho_1\rho_2\rho_1^{-1}$

$= \rho_1\rho_2\rho_2$

$= \rho_1\rho_1 = \rho_2 \in A_3$

$\mu_2\rho_1\mu_2^{-1}$

$= \mu_3\mu_2 = \rho_2 \in A_3$ ✓

and S_3/A_3 is cyclic

$(|S_3/A_3| = 6/3 = 2)$

therefore abelian.

$\therefore \quad C = A_3$.

Group Action on a Set

def Let X be a set, G be a group.

Action of G on X is a map $*: G \times X \to X$ s.t.

1. $ex = x$; $\forall x \in X$
2. $(g_1g_2)(x) = g_1(g_2x)$; $\forall x \in X, \forall g_1, g_2 \in G$.

multiplication as function composition.

$\therefore$ X is a G-set

Thm Let X be G-set. $\forall g \in G$: $\sigma_g : X \to X$: $\sigma_g(x) = gx$. ; $x \in X$ = perm. of X.

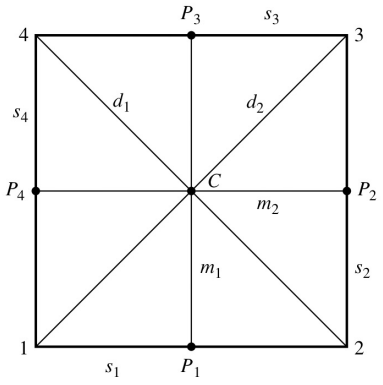
$\phi : G \to S_X$: $\phi(g) = \sigma_g$ is a homomorphism that $\phi(g)(x) = gx$.

* Group action is faithful if $g = e$ is the only element that leaves $gx = x$.
* G is transitive on G-set X if $\forall x_1, x_2 \in X$, there exists $g \in G$ s.t. $gx_1 = x_2$.

Isotropy Subgroups

$X_g = \{x \in X : gx = x\}$, $G_x = \{g \in G : gx = x\}$

e.g. $G = D_4$, X is a set.



16.9 Figure

16.10 Table

	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_0	1	2	3	4	s_1	s_2	s_3	s_4	m_1	m_2	d_1	d_2	C	P_1	P_2	P_3	P_4
ρ_1	2	3	4	1	s_2	s_3	s_4	s_1	m_2	m_1	d_2	d_1	C	P_2	P_3	P_4	P_1
ρ_2	3	4	1	2	s_3	s_4	s_1	s_2	m_1	m_2	d_1	d_2	C	P_3	P_4	P_1	P_2
ρ_3	4	1	2	3	s_4	s_1	s_2	s_3	m_2	m_1	d_2	d_1	C	P_4	P_1	P_2	P_3
μ_1	2	1	4	3	s_1	s_4	s_3	s_2	m_1	m_2	d_2	d_1	C	P_1	P_4	P_3	P_2
μ_2	4	3	2	1	s_3	s_2	s_1	s_4	m_1	m_2	d_2	d_1	C	P_3	P_2	P_1	P_4
δ_1	3	2	1	4	s_2	s_1	s_4	s_3	m_2	m_1	d_1	d_2	C	P_2	P_1	P_4	P_3
δ_2	1	4	3	2	s_4	s_3	s_2	s_1	m_2	m_1	d_1	d_2	C	P_4	P_3	P_2	P_1

$X = \{1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, C, P_1, P_2, P_3, P_4\}$.

- $X_{\rho_0} = X$, $X_{\rho_1} = \{C\}$, $X_{\mu_1} = \{s_1, s_3, P_1, P_3, C, m_1\}$ → $x \in X_{\mu_1}$ อยู่ที่เดิมเมื่อทำ μ_1 ($\mu_1 x = x$)
- $G_1 = \{\rho_0, \delta_2\}$, $G_{s_3} = \{\rho_0, \mu_1\}$, $G_{d_1} = \{\rho_0, \rho_2, \delta_1, \delta_2\}$

Thm X is G-set. $G_x \leq G$; $\forall x \in G$ ↳ d_1 อยู่ที่เดิมเมื่อทำ $g \in G_{d_1}$ ($g d_1 = d_1$)

def From Thm, $G_x \leq G$ is the isotropy subgroup of x.

Orbits

Thm Let X be G-set. $x_1, x_2 \in X$: $x_1 \sim x_2 \leftrightarrow gx_1 = x_2$; $\exists g \in G$.
↳ $\sim$ ≡ equivalence relation on X.

def Let X be G-set.

Orbit of x : Gx (or $G \cdot x$) $= \{gx : g \in G\}$
↳ Set of elements in X to which x can be moved by the elements of G.

Thm Let X be G-set. $|Gx| = (G : G_x) = \dfrac{|G|}{|G_x|}$; $|Gx| \mid |G|$. (If finite.)

e.g., from D_4, $G1 = \{1, 2, 3, 4\}$.
↳ 1 can be moved to 2 or 3 or 4 or 1 (not moved at all.)

⊕ Stabilizer of x ≡ All S_G which sends x to itself ($\{\sigma : \sigma(x) = x\}$)

In Counting

Thm (Burnside's Formula) Let G be finite group, X be G-set.

r is the number of orbits in X under G:

$$|X/G| = r \cdot |G| = \sum_{g \in G} |X_g|$$

---

④ Rings & Fields

closure of multiplication.

def A Ring $\langle R, +, \cdot \rangle$ is a set R with two binary operations: $+, \cdot$ s.t.

- $\mathcal{R}1$: $\langle R, + \rangle$ is an abelian group.
- $\mathcal{R}2$: $\cdot$ is associative.
- $\mathcal{R}3$: Has left & right distributive law: $\begin{cases} a \cdot (b+c) = a \cdot b + a \cdot c, \\ (a+b) \cdot c = a \cdot c + b \cdot c. \end{cases}$

* We can write $a \cdot b$ as ab, and, $\langle R, +, \cdot \rangle$ as R.
* $M_n(V)$; $V \subseteq \mathbb{C}$, is a Ring.
* $V \subseteq \mathbb{C}$ is a Ring, e.g. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \ldots$
* $n\mathbb{Z}$ is a Ring.
* $\mathbb{Z}_n$ is a Ring.
* $R_1 \times R_2 \times \ldots \times R_n \equiv$ direct product of R_i.

Thm If R is a ring with additive identity "0", then $\forall a, b \in R$:

1. $0a = a0 = 0$
2. $a(-b) = (-a)b = -ab$
3. $(-a)(-b) = ab$

Homomorphisms & Isomorphisms

def $\phi : R \to R'$ is homomorphism if 1. $\phi(a+b) = \phi(a) + \phi(b)$ $(\phi : \langle R, + \rangle \to \langle R', + \rangle)$

2. $\phi(ab) = \phi(a)\phi(b)$ $(\phi : \langle R, \cdot \rangle \to \langle R', \cdot \rangle)$

ϕ is 1-1 if $\ker(\phi) = \{a \in R : \phi(a) = 0'\} = \{0\}$.

Evaluation homomorphism : $\phi_p : F \to \mathbb{R}$: $\phi_a(f) = f(a)$ for $f \in F$; $F : \mathbb{R} \to \mathbb{R}$

def Isomorphism $\phi : R \to R'$ is a 1-1 homomorphism. $\longrightarrow R \simeq R'$.

* Zero Ring $\{0\}$ where $0+0=0$,
$0 \cdot 0 = 0$,
0 is both additive & multiplicative identity.

def A ring with commutative multiplication is commutative ring.

A ring with multiplicative identity is ring with unity. (identity 1 is "unity")

* unity $1 \neq 0 \rightarrow$ there is multiplicative inverse.

def Let R be ring with unity $1 \neq 0$.

$u \in R$ is a unit of R if it has multiplicative inverse in R.

* If every nonzero $\in R$ is a unit, then R is division ring (skew field)

def A Field F is commutative division ring. (Ring with identity, inverse, commutativity of multiplication. (2^{nd} bin. op.))

* Strictly skew field is noncommutative division ring.

def $a \in R$ is idempotent if $a^2 = a$.

def $a \in R$ is nilpotent if $a^n = 0$; $\exists n \in \mathbb{Z}^+$.

def R_a is a subring generated by a.

def R is a Boolean ring if $a^2 = a$; $\forall a \in R$. e.g., $\mathbb{Z}_2 = \{0, 1\}$.

Integral Domains

Problem: In $\mathbb{Z}_{12}$, $2\cdot 6 = 6\cdot 2 = 3\cdot 4 = 4\cdot 2 = \dots = 8\cdot 9 = 9\cdot 8 = 0$.

def If a, b are nonzero element in R s.t. $ab = 0$,
then a, b are **0-divisors** (**divisors of 0**).

e.g. In $\mathbb{Z}_{12}$, $2, 3, 4, 6, 8, 9, 10$ are divisors of 0 and $\gcd(\_, 12) \neq 1$.

Thm In ring $\mathbb{Z}_n$, divisors of 0 are nonzero $a \in \mathbb{Z}_n$ which $\gcd(a, n) \neq 1$.

Col If p is prime, $\mathbb{Z}_p$ has no divisors of 0.

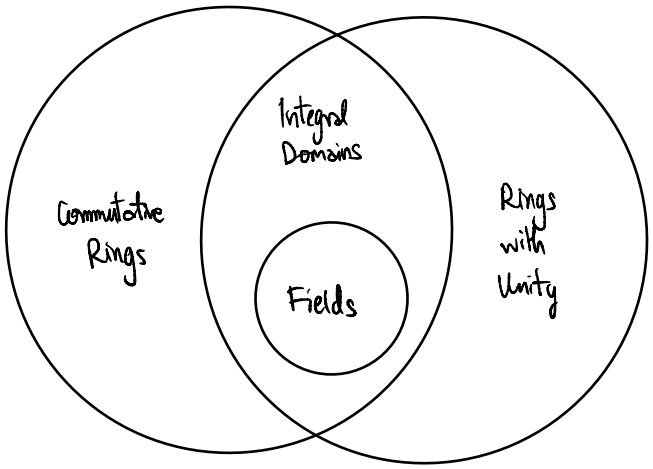
* **Cancellation laws** in R: $ab = ac \wedge a \neq 0 \rightarrow b = c$.

Thm Cancellation laws hold in $R \longleftrightarrow R$ has no divisors of 0.

def **Integral Domain** D is a commutative ring with unity $1 \neq 0$
and containing no divisors of 0.

e.g. $\mathbb{Z}$, $\mathbb{Z}_p$ are integral domains.

Thm Every field F is an integral domain.



Thm Every finite integral domain is a field.

Col If p is prime, $\mathbb{Z}_p$ is a field.

Characteristic of a Ring

def Ring R, if there exists positive integer n s.t. $n \cdot a = 0 \quad \forall a \in R$,
then ring R is of characteristic n. Else, R is of characteristic 0.

e.g. $\mathbb{Z}_n$ is of characteristic n.
$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ have characteristic 0.

Thm Let R be a ring with unity. If $n \cdot 1 \neq 0 \; ; \forall n \in \mathbb{Z}^+$, R has characteristic 0.
If $n \cdot 1 = 0 \; ; \exists n \in \mathbb{Z}^+$, smallest n is charac. of R.

Thm (Little Theorem of Fermat) $a^{p-1} \equiv 1 \pmod p$

↓

Col $a^p \equiv a \pmod p$

↓

Merseme Primes : $2^p - 1$

Euler's Generalization

$\mathbb{Z}_n^*$

Thm Let G_n = set of nonzero elements of $\mathbb{Z}_n$ which are not 0-divisors.
$\langle G_n, \cdot_n \rangle$ is a group. ($a \cdot_n b = ab \bmod n$)

* Euler phi-function $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+ ; \varphi(n) = |G_n|$ → $\varphi(n) = \#a \; ; \; \gcd(a,n) = 1, a \leq n$.

Thm (Euler's Thm) $a^{\varphi(n)} \equiv 1 \pmod n \; ; \; \gcd(a,n) = 1$.

Thm Let $m \in \mathbb{Z}^+, a \in \mathbb{Z}_m, \gcd(a,m) = 1$.
For each $b \in \mathbb{Z}_m$, $ax = b$ has a unique solution $x \in \mathbb{Z}_m$

Col $\gcd(a,m) = 1 \rightarrow$ Any b : $ax \equiv b \pmod m$ has sol. be all integers in residue class mod m.

Thm Let $m \in \mathbb{Z}^+$, $a, b \in \mathbb{Z}_m$, $d = \gcd(a, m)$.

$ax = b : x \in \mathbb{Z}_m \leftrightarrow d \mid b$. → eqn. has d solutions in $\mathbb{Z}_m$.

e.g. $\mathbb{Z}_8$ $\quad 2x = 6$, $d = 2$, $2 \mid 6$ → $x = 3, 7$.

e.g. $15x \equiv 27 \pmod{18} \leftrightarrow 5x \equiv 9 \pmod{6} \leftrightarrow$ Solve $5x = 3$ in $\mathbb{Z}_6$ ∴

Field of Quotients of Integral Domain

D: 1. Define elements of F.

2. Define bin. op. of $+, \cdot$ on F.

3. check if F is a field under $+, \cdot$

4. Show that F can be viewed as containing D as integral subdomain.

1.) Let D be Integral Domain. : $D \times D = \{(a, b) : a, b \in D\}$

Pair $(a, b) \mapsto a/b$: $S \subseteq D \times D$: $S = \{(a, b) : a, b \in D,\ b \neq 0\}$

* $(2, 3)$ and $(4, 6)$ are equivalent.

def $(a, b) \sim (c, d) \leftrightarrow ad = bc$. $\left(\frac{a}{b} = \frac{c}{d}\right)$

└* is an equivalence relation ∵ reflexive, symmetric, transitive.

We then def $[(a, b)]$ be equivalence class of (a, b) in S under $\sim$.

We let F = Set of every $[(a, b)]$ for $(a, b) \in S$.

2.) Define $\cdot, +$: If $D = \mathbb{Z}$, $[(a, b)] : \frac{a}{b} \in \mathbb{Q}$

Lemma : for $[(a, b)], [(c, d)]$ in F, $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$

$[(a, b)][(c, d)] = [(ac, bd)]$.