

Sets.

Relations.

Groups.

I. Sets

1.1. Basic set properties.

cardinality : # of elmts in a set.

↳ $|A|$ or $n(A)$.

1.3. Subset

$$A \subseteq B \Leftrightarrow \forall x \in A \Rightarrow x \in B.$$

$$\begin{array}{l|l} \text{e.g. } \{\emptyset\} \in \{\{\emptyset\}\} & \{x\} \subseteq \{x, y, z\} \\ \emptyset \subseteq \{\{\emptyset\}\} & \{x\} \subset \{x, y, z\} \\ \{\emptyset\} \not\subseteq \{\{\emptyset\}\} & \{x\} \not\subset \{x, y, z\} \end{array}$$

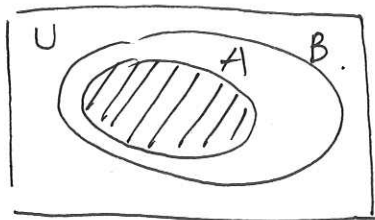
$$* \{\emptyset\} \neq \emptyset$$

1.2. Venn Diagrams

* \sim "contra-positive".

$$A \Rightarrow B \text{ . (A inside B).}$$

$$\neg B \Rightarrow \neg A \text{ (} \forall \text{ elmt not in B} \Rightarrow \text{not in A)}$$



1.4. Power Set

Def. $P(A) = \{X \mid X \subseteq A\}$.

\uparrow
the set of all subsets of A .

Thm

$$|A| = n \Rightarrow |P(A)| = 2^n.$$

[proof by binomial thrm]

1.5. Operation on sets.

disjoint sets : $A \cap B = \emptyset$

property.

• Associativity.

• Distributivity.

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

• Commutative.

$$\bigcup_{i=1}^n A_i \quad \bigcap_{i=1}^n A_i.$$

1.6 Set Differences

Def. $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$.

$$A' = \{x \mid x \in U \text{ and } x \notin A\}$$

$$* A \setminus B = A \cap B'$$

symmetric difference

$$A \Delta B = \{x \mid x \in (A \cup B) \text{ and } x \notin (A \cap B)\}.$$

$$= (A \cup B) \setminus (A \cap B)$$

$$= (A \setminus B) \cup (B \setminus A)$$

De Morgan's laws

$$(A \cup B)' = A' \cap B'$$

$$(A \cap B)' = A' \cup B'$$

II Relations.

2.1. Relations.

- The Cartesian product.

Def. $A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$.

- Relations

Notation:

- If R is a relation, $(x, y) \in R \leftrightarrow xRy$.

- Equivalence relations

def. A relation R on a set M is reflexive, iff $(x, x) \in R$. or, equivalently $xRx \quad \forall x \in M$.

e.g. $S = \{(a, b) \in \mathbb{N}^2 \mid ab \geq 0\}$. is reflexive.

def. R is symmetric iff:

$\forall x, y \in M, (x, y) \in R \Rightarrow (y, x) \in R$.
or equivalently.

$xRy \Rightarrow yRx \quad \forall x, y \in M$.

e.g. $S = \{(a, b) \in \mathbb{N}^2 \mid ab \geq 0\}$ is symmetric.

Def.

R on a set M is antisymmetric.

iff $\forall x, y \in M$,

$(x, y) \in R$ and $(y, x) \in R \Rightarrow x = y$.

i.e. $\forall x, y \in M$,

xRy and $yRx \Rightarrow x = y$.

e.g. $\rho = \{(x, y) \in \mathbb{R}^2 \mid x \geq y\}$.

Def.

R is transitive iff:

$\forall x, y, z \in M, (x, y) \in R, (y, z) \in R \Rightarrow (x, z) \in R$;

i.e. $\forall x, y, z \in M, xRy$ and $yRz \Rightarrow xRz$.

e.g. $\gamma = \{(x, y) \in \mathbb{R}^2 \mid x \geq y\}$.

Def.

R on set M is an equivalence relation if it is reflexive, symmetric and transitive.

Equivalence classes.

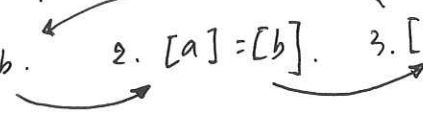
def. if R is an equivalence relation on a set A for $a \in A$, the set $[a] = \{x \in A \mid xRa\}$ of elmts of A which are equiv. to a is called the equiv. class of a w/ respect to R , (R -equiv. class of a).

Thrm

if R is an equiv. relation on a set A , then any 2 equiv. classes. $[a]$ and $[b]$ are either disjoint, or if they have any elmt in common then they must be equal.

i.e. the 3 statements are equiv.:

1. aRb . 2. $[a] = [b]$. 3. $[a] \cap [b] \neq \emptyset$



\Rightarrow Remark:

$[a] \neq [b]$ iff. $[a] \cap [b] = \emptyset$.

def. A partition of a set A is a collection of
① non-empty, ② disjoint subsets of A that are
③ mutually exhaustive.

i.e. a collection of n non-empty subsets of A s.t.

$$A_i \cap A_j = \emptyset, \forall i \neq j, \text{ and } \bigcup_{i=1}^n A_i = A.$$

$$\Rightarrow [a_i] \neq \emptyset$$

$$\bigcup_{i=1}^n [a_i] = A.$$

$$[a_i] \cap [a_j] = \emptyset, \forall i \neq j.$$

i.e. equiv. relation created a partition of the set A whose subsets are the equiv. classes.

Thrm

if R is an equiv. relation on a set A , then the equiv. classes of R induce a partition of set A .

Proof:

1. the equiv. classes form a partition of set A .
2. A partition of set A forms an equiv. relation on set A .

Congruence

def. $a \equiv b \pmod{m} \Leftrightarrow m \mid (a-b)$
 $a \not\equiv b \pmod{m} \Leftrightarrow m \nmid (a-b)$
 m is the modulus of congruence.

Thrm

Let $m \in \mathbb{Z}^+$. Then congruence modulo m is an equiv. relation.

2.2. Functions.

def. if A and B are non-empty sets.
a function from A to B is a relation f from A to B . s.t. $\forall x \in A$, there is a unique elmt $y \in B$ w/ $(x, y) \in f$.

Note: $f: A \rightarrow B$.

$\Leftrightarrow f: x \mapsto y, x \in A, y \in B$.
(\rightarrow for sets; \mapsto for elmts)

- A is domain; B is codomain.
- y is the image of x under f . / x is mapped to $y = f(x)$ by the function f .
- x : input / preimage
 y : output.

def. the subset of B defined by $\{f(a) \mid a \in A\}$ is the image of A . and is denoted $f(A)$.
i.e. the image of A is the subset of B that consists of the images of all elmts of A .

Remark If $f(A) = B$, then B is the range of f .

def. $f: A \rightarrow B$ is a surjection
 $\Leftrightarrow \forall y \in B, \exists$ at least one $x \in A$ s.t. $f(x) = y$.

def. $f: A \rightarrow B$ is an injection
 $\Leftrightarrow \forall x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$
(distinct inputs of f produce dist. outputs)

Remark:

The def is equiv. to:

- $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
(Contra positive).
- $\forall y \in f(A). \exists! x \in A$ s.t. $f(x) = y$.
- $\forall y \in \text{Codomain}. \exists$ at most one $x \in A \dots$

Note: if f is injective,
 $n(A) \leq n(B)$. or, $|A| \leq |B|$.

Def. $f: A \rightarrow B$ is a bijection

$\Leftrightarrow f$ is both an injection and surjection.

Remark:

surjection: $|A| \geq |B|$.

injection: $|A| \leq |B|$

\Rightarrow bijection: $|A| = |B|$

Def. $i_A: A \rightarrow A$ defined by $i_A(x) = x, \forall x \in A$
if known as the identity function.

Composition of functions

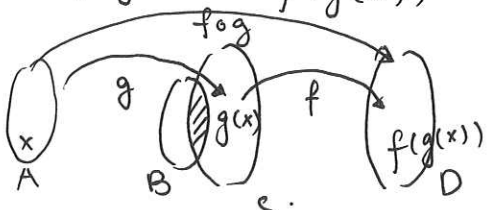
* the outputs of g must be elmts of domain of f .

i.e. the range of g is a subset of the domain of f .

Def. $g: A \rightarrow B, f: C \rightarrow D, g(A) \subseteq C$.

$f \circ g$: $A \rightarrow D$ defined by

$$f \circ g(x) = f(g(x))$$



Note:

the composition is not commutative, but is associative.

$$\text{i.e. } (f \circ g) \circ h = f \circ (g \circ h).$$

Inverse Functions

Def. $R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in A \times B\}$

$\Leftrightarrow y R^{-1} x$ iff. $x R y$.

Note: Reflection w/ respect to line $y=x$.
(first bisector / identity line).

Note: The inverse relation of f may not be a function.

If it is, it's the inverse function of f , denoted by f^{-1} . $f^{-1}(y) = x$ when $f(x) = y$.

Thrm

Note: the function have to be a bijection in order to have an inverse function.

$$\text{Note: } f \circ f^{-1}(y) = y \Rightarrow f \circ f^{-1} = i_B.$$

$$f^{-1} \circ f(x) = x \Rightarrow f^{-1} \circ f = i_A.$$

This is a method to test whether 2 functions are inverses.

III Groups (I)

3.1. Binary Operations.

Definition 1

A binary operation on a set A is a function from $A \times A$ into A . Thus, it is a rule $*$ which assigns to every ordered pair $(a, b) \in A \times A$ exactly one element $c \in A$; denoted by $a * b = c$.

Remark:

- The rule for the operation must be well-defined: must assign to every ordered pair (a, b) exactly one elmt c .
- $c \in A$. (closure property)

properties of binary operations

def 2.

A binary operation $*$ on a set G is:

- associative $\Leftrightarrow \forall a, b, c \in G$,
 $a * (b * c) = (a * b) * c$.
- commutative. $\Leftrightarrow a * b = b * a$
- distributive over $\Delta \Leftrightarrow$
 $a * (b \Delta c) = (a * b) \Delta (a * c)$

operation (Cayley) tables

Note: To see if a group is commutative, check if the table is symmetric about the main diagonal.

the identity elmt.

def 3. A elmt e in a set S is an identity elmt for an operation Δ defined over S if $e \Delta a = a \Delta e = a. \quad \forall a \in S$.

(there's also right & left-identity)

Thrm 1

if an operation \circ admits a left-identity e_1 and a right identity e_2 , then these identities are equal.

Thrm 2.

If $*$ on a set S admits an identity elmt e , then this elmt is unique.

the inverse elmt.

Def. 4

$$a^{-1} \Delta a = a \Delta a^{-1} = e. \quad \forall a \in S.$$

\uparrow left \uparrow right.

Thrm 3 If, for an associative operation \circ , an elmt a admits a left-inverse a' and a right a'' , then $a' = a''$.

Thrm 4 If an operation $*$ defined on a set S has an identity elmt. e , then every invertible elmt admits a unique inverse.

Cancellation Rules

Thrm 5.

if $a * b = a * c$, then $b = c$.
if $b * a = c * a$, then $b = c$.

3.2 Groups.

def 5. $(G, *)$:

1. closure: $a * b \in G$.
2. Associativity: $(a * b) * c = a * (b * c)$.
3. identity: $\exists e$ st. $a * e = e * a = a$.
4. Inverses: $\exists b$. s.t. $a * b = b * a = e$.

* Abelian/Commutative: $a * b = b * a$.

* order $|G|$ $\begin{cases} \text{finite} \\ \text{infinite} \end{cases}$.

Thrm 6 (Latin square property)

$\forall a, b \in (G, *)$, $\exists!$ c . s.t. $a * c = b$.

Thrm 7

If a and b are elmts of $(G, *)$. then.

1. $(a^{-1})^{-1} = a$
2. $(a * b)^{-1} = b^{-1} * a^{-1}$

Note

$$a^0 = e.$$

Congruence revisited

Def 6

$[a] = \{x \mid x \in \mathbb{Z} \text{ and } x \equiv a \pmod{n}\}$
 $a \in \mathbb{Z}, n \in \mathbb{Z}^+$.

Theorem 8

$$a \equiv b \pmod{n} \Leftrightarrow [a] = [b]$$

Thrm 9

There are n diff. congruence classes.

Def 7.

The set of all congruence classes modulo n is denoted $\mathbb{Z}_n = \{[0], [1] \dots [n-1]\}$.

Thrm 10

Let $a, b, c, d \in \mathbb{Z}$, $m \in \mathbb{Z}^+$.

$$a \equiv b \pmod{m}, \quad c \equiv d \pmod{m}$$

$$\Rightarrow \begin{aligned} 1. & a \pm c \equiv b \pm d \pmod{m} \\ 2. & ac \equiv bd \pmod{m} \end{aligned}$$

Remark: if $\gcd(c, m) = 1$,
then $ac \equiv bc \pmod{m}$
 $\Rightarrow a \equiv b \pmod{m}$.

Thrm 11

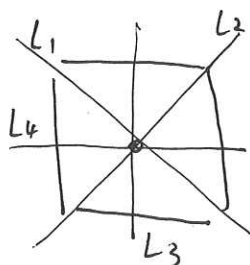
$$[a] = [b], [c] = [d] \text{ in } \mathbb{Z}_n.$$

$$\Rightarrow [a+c] = [b+d], [ac] = [bd].$$

Def 8.

$$\text{In } \mathbb{Z}_n: [a] + [c] = [a+c]$$

$$[a][c] = [ac].$$



More Groups.

Symmetries of a square.

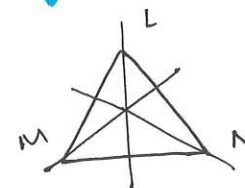
$$(D_4, \circ) \text{ w/ operation}$$

$$D_4 = \{e, r, r^2, r^3, L_1, L_2, L_3, L_4\}$$

Symmetries of an equilateral triangle.

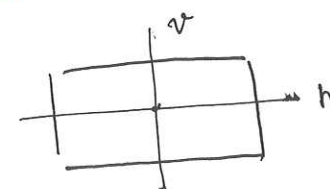
$$(D_3, \circ)$$

$$D = \{I, R, R^2, L, M, N\}$$



Symmetries of a rectangle.

$$(\{e, r, h, v\}, \circ).$$



3.3. Permutations

Def 9.

A Permutation on a set S is a bijection

$\alpha: S \rightarrow S$. The set of all permutations on S is denoted S_n .

If $\alpha, \beta \in S_n$, we simplify $\alpha \circ \beta$ as $\alpha\beta$.

Remark

if $\alpha, \beta, \gamma \in S_n$:

$$1. \alpha\beta \in S_n.$$

$$2. \alpha(\beta\gamma) = (\alpha\beta)\gamma.$$

$$3. \alpha^{-1} \in S_n.$$

4. The identity function e is in S_n .

IV Group (II)

4.1. Introduction.

Def. 1 $a \in (G, *)$ has finite order if

$$a^m = e \text{ for some } m \in \mathbb{Z}^+.$$

\Rightarrow order of elmt a is $|a|$.

$a \in (G, *)$ has infinite order
if $a^m \neq e$ for every $m \in \mathbb{Z}^+.$

Thrm 1

$$a \in (G, \cdot).$$

1. if a has finite order n , then $a^m = e$

$$\Leftrightarrow n \mid m.$$

$$2. a^p = a^q \Leftrightarrow p \equiv q \pmod{n}$$

3. If a has infinite order,
 $a^i \neq a^j$ when $i \neq j$.

Remark:

1. if $|a| = n$. $n = kr$: $r > 0$

$$\Rightarrow |a^r| = k.$$

2. if $a^x = a^y$. $x \neq y$

$\Rightarrow a$ must have a finite order.

4.2. Subgroups

Def 2.

if a non-empty subset H of G is
itself a group under the same operation,

$\begin{cases} H \subset G, & \text{proper subgroup} \\ H \subseteq G, & \text{subgroup.} \end{cases}$

• trivial subgroup:

$$(\{e\}, *)$$

Also, $(G, *)$.

Aside from these two, all are proper.

Thrm 2.

$X = \{x^k \mid k \in \mathbb{Z}\} \subseteq (G, *)$ for $x \in G$.
 X is the cyclic subgroup generated
by x . x is the generator of the
subgroup.

Subgroup tests.

Thrm 3

$$H \subseteq G \text{ iff } ab^{-1} \in H. \quad \forall a, b \in H.$$

[proof by using identity. inverse. closure axiom]

Thrm 4

$$H \subseteq G \text{ iff.} \quad \swarrow \text{closure.}$$

$$1. ab \in H. \quad \forall a, b \in H, \text{ and}$$

$$2. a^{-1} \in H. \quad \forall a \in H \quad \nwarrow \text{Inverse.}$$

Thrm 5 (Finite @ Subgroup test)

$$H \subseteq G. \quad (H \text{ is finite.}) \text{ if.}$$

H is closed under operation of G .

The center of a group

$$C(G) = \{a \in G : ag = ga \quad \forall g \in G\}.$$

Thrm $C(G)$ is a ~~st~~ subgroup of G .

⇒ Permutation Group on S

S_n is the symmetric Group on n elmts.

Remark:

There are $n!$ permutations of a set of n objects.

Notation

Two-row notation (array notation)

e.g. $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}$.

* Each member of the first row is mapped onto the corresponding member in 2nd row.

Product of permutations

* $\alpha\beta: \forall \beta \in \alpha$.

* $\alpha\beta \neq \beta\alpha$.

* $e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$.

* $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}$.

Cycle notation.

$\alpha = (1532)(4)$.

* permutations that do not move any items are written as (1) .

product of permutations using cycle notation.

e.g. $(1342)(3645)(1623)$.

$$\begin{cases} 1 \rightarrow 6 \rightarrow 4 \rightarrow 2 \therefore 1 \rightarrow 2 \\ 2 \rightarrow 3 \rightarrow 6 \rightarrow 6 \therefore 2 \rightarrow 6 \\ 6 \rightarrow 2 \rightarrow 2 \rightarrow 2 \therefore 6 \rightarrow 1 \end{cases} \therefore (126)$$

$3 \rightarrow 1 \rightarrow 1 \rightarrow 3 \therefore 3 \rightarrow 3 \therefore 3$ is fixed.

$$\begin{cases} 4 \rightarrow 4 \rightarrow 5 \rightarrow 5 \therefore 4 \rightarrow 5 \\ 5 \rightarrow 5 \rightarrow 3 \rightarrow 4 \therefore 5 \rightarrow 4 \end{cases} \therefore (45)$$

⇒ $(126)(45)$

Inverse of a permutation.

* $\alpha = (1573)(468)$.

⇒ $\alpha^{-1} = (864)(3752)$. → Cycle form.

* Swap R_1 and R_2 , rearrange the new R_1 .

→ Array form.

Inverse of a product of permutations

* permutation is a function.

Thm

$$(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}.$$

* Cancellation law is valid.

$$\text{i.e. } \alpha\beta = \alpha\gamma \Leftrightarrow \beta = \gamma.$$

* Order of a permutation.

Def For any permutation α , $\exists n \in \mathbb{Z}^+$.

s.t. $\alpha^n = e$. the smallest n is the order.

denoted. $\text{ord}(\alpha) = n$.

Thm

The order of a permutation written in disjoint cycle form is the lcm of length of the cycles.

$$\text{e.g. } \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} = (132)(45).$$

$$\text{ord}(\alpha) = \text{lcm}(2, 3) = 6.$$

Summary of properties of permutations.

- If disjoint cycle form of α has no number in common w/ the disjoint cycle form of β . the α . β commute.