Review: Sets and Equivilance Relations

Def) A set X is a well-defined collection of objects

For any object x we can decide if $x \in X$ or $x \notin X$.

Ex) $\mathbb{Q} = \{ \frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0 \}$

Subsets

$A \subseteq B$, $A \subset B$

$A \not\subseteq B$

$\emptyset$ - Empty set

Set operations

unions $= A \cup B = \{ x \mid x \in A$ or $x \in B \}$

$$\bigcup_{i=1}^{n} A_i = A_1 \cup \cdots \cup A_n$$

Intersection $A \cap B = \{ x \mid x \in A$ and $x \in B \}$

$$\bigcap_{i=1}^{n} A_i$$

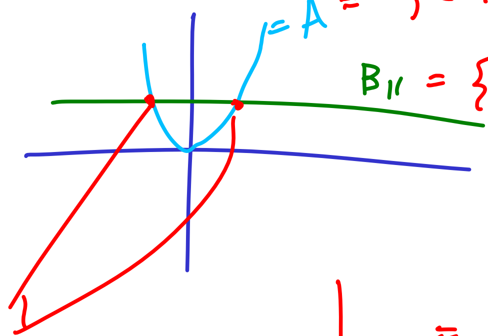
Disjoint if $A \cap B = \emptyset$

Suppose $A \subseteq U$

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

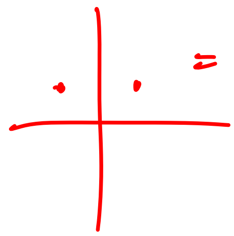
Difference : $A \setminus B = A \cap B' = \{x \mid x \in A, x \notin B\}$

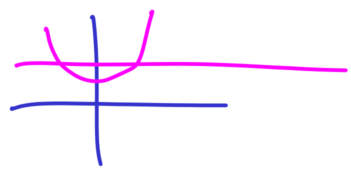
$U = \mathbb{R}^2$



$= A = \{(x,y) \mid y = x^2\}$

$B_{11} = \{(x,y) \mid y = 1\}$

$A \cap B =$  $= \{(1,1), (-1,1)\}$

$A \cup B =$ 

Proposition 1.2. *Let A, B, and C be sets. Then*

1. $A \cup A = A$, $A \cap A = A$, *and* $A \setminus A = \emptyset$;
2. $A \cup \emptyset = A$ *and* $A \cap \emptyset = \emptyset$;
3. $A \cup (B \cup C) = (A \cup B) \cup C$ *and* $A \cap (B \cap C) = (A \cap B) \cap C$;
4. $A \cup B = B \cup A$ *and* $A \cap B = B \cap A$;
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Theorem 1.3 (De Morgan's Laws). *Let A and B be sets. Then*

1. $(A \cup B)' = A' \cap B'$;
2. $(A \cap B)' = A' \cup B'$.

Cartesian Product :

$A \times B = \{(a,b) \mid a \in A, b \in B)$

Mappings

A <u>mapping</u> or <u>function</u> from A to B is a relation

$$f = \{ (a, b) \mid \text{for } \forall a \in A \ \exists \text{ unique } b \in B \}$$

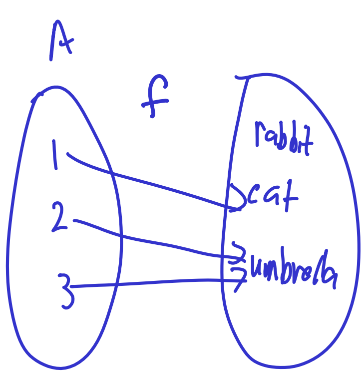
Note:

- Not all $b \in B$ need appear
- different $a_1, a_2 \in A$ can pair with the same b just not with multiple b.

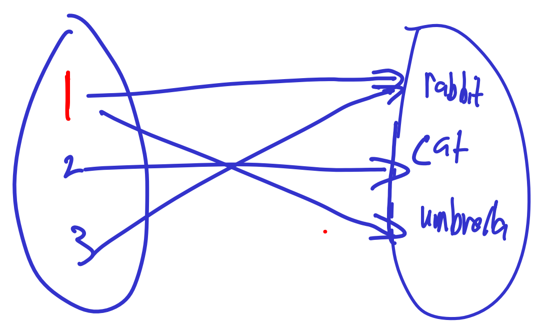
$$f : A \to B \quad \text{or} \quad A \xrightarrow{f} B$$

$$f(a) = b \quad \text{or} \quad f : a \mapsto b \quad \left(\text{instead of } (a,b) \in f \subseteq A \times B \right)$$

Ex)



This <u>is</u> a function



Not a function

A relation can fail to be a function if it is <u>not</u> well-defined

A relation is <u>well-defined</u> if each element in the domain is assigned to a <u>unique</u> element in the range

Ex) $f: \mathbb{Q} \to \mathbb{Z}$ is Not well defined

$\frac{p}{q} \mapsto p$

$\frac{1}{2} = \frac{2}{4}$

$f(\frac{1}{2}) = 1$
$\nparallel$
$f(\frac{2}{4}) = 2$

Onto / Surjective : $f(A) = B$, i.e. $\exists\, a \in A$ for each $b \in B$ s.t. $f(a) = b$

injective / 1-1 : $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$

If $f(a_1) = f(a_2) \Rightarrow a_1 = a_2$

Bijective = 1-1 and onto

Ex) $f: \mathbb{Z} \to \mathbb{Q}$

$n \mapsto \frac{n}{1}$ is 1-1 but Not onto

$g: \mathbb{Q} \to \mathbb{Z}$

$: \frac{p}{q} \to p$ where $\frac{p}{q}$ is expressed in lowest terms and $q > 0$

is onto Not 1-1

composition:

$f: A \to B$, $g: B \to C$

$g \circ f : A \to C$

$: x \mapsto g(f(x))$

Theorem 1.15. *Let $f : A \to B$, $g : B \to C$, and $h : C \to D$. Then*

1. *The composition of mappings is associative; that is, $(h \circ g) \circ f = h \circ (g \circ f)$;*
2. *If f and g are both one-to-one, then the mapping $g \circ f$ is one-to-one;*
3. *If f and g are both onto, then the mapping $g \circ f$ is onto;*
4. *If f and g are bijective, then so is $g \circ f$.*

Identity

$$id_S : S \to S$$
$$: s \mapsto s$$

A map $g : B \to A$ is an inverse mapping of $f : A \to B$

if $g \circ f = id_A$ and $f \circ g = id_B$

write $g = f^{-1}$

Ex) Suppose $S = \{1, 2, 3\}$ define a map

$\pi : S \to S$

$$\pi(1) = 2, \quad \pi(2) = 3, \quad \pi(3) = 1$$

π is bijective

$$\begin{pmatrix} 1 & 2 & 3 \\ \pi(1) & \pi(2) & \pi(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (2\,3\,1)$$

$$\pi^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\pi^{-1} : 2 \mapsto 1, \quad \pi^{-1} : 3 \mapsto 2, \quad \pi^{-1} : 1 \to 3$$

Theorem A mapping is invertible if it is both 1-1 and onto.

Equivilence Relations

An equivalence relation $\sim$ on a set X is a relation $R \subseteq X \times X$

- $(x, x) \in R \quad \forall x \in X$ (reflexive property)

  $x \sim x$

- $(x, y) \in R \Rightarrow (y, x) \in R$ (symmetric property)

  $x \sim y \Rightarrow y \sim x$

- $(x, y) \in R$ and $(y, z) \in R \Rightarrow (x, z) \in R$

  $x \sim y$ and $y \sim z \Rightarrow x \sim z$. [transitive property]

A partition P of set X is a collection of non-empty sets $X_1, X_2, \dots,$ s.t. $X_i \cap X_j = \emptyset$ for $i \neq j$

and $\bigcup_k X_k = X$

Equivlence class

$$[x] = \{ y \in X \mid y \sim x \}$$

Theorem 1.25. *Given an equivalence relation $\sim$ on a set X, the equivalence classes of X form a partition of X. Conversely, if $\mathcal{P} = \{X_i\}$ is a partition of a set X, then there is an equivalence relation on X with equivalence classes X_i.*

Cor] Two Eq. Classes are either disjoint or equal

Ex] Let r, s be in $\mathbb{Z}$ suppose $n \in \mathbb{N}$ $n > 0$

r is congruent to s modulo n

or

$r \equiv s \pmod{n}$ if

$r - s = n \cdot k$ for some $k \in \mathbb{Z}$

(alt. $r - s$ is divisible by n)

Ex. $41 \equiv 17 \pmod{8}$ since $41 - 17 = 24 = 8 \cdot 3$

Congruence mod n is an Eq. relation on $\mathbb{Z}$.

- $r \equiv r \pmod{n}$ since $r - r = 0 = 0 \cdot n$ ✓ (reflexive)
- $r \equiv s \pmod{n} \Rightarrow r - s = n \cdot k$ (symmetric)
  $\Rightarrow s - r = n(-k) \Rightarrow s \equiv r \pmod{n}$
- $r \equiv s \pmod{n}$ and $s \equiv t \pmod{n}$

$\Rightarrow \quad r-s = kn \quad$ ant $\quad s-t = l\cdot n \qquad (k, l \in \mathbb{Z})$

$$r-s + s-t = kn + ln$$

$$r-t = n(k+l) \Rightarrow r \equiv t \pmod{n}$$

$\mathbb{Z}/3\mathbb{Z}$ = integers modulo 3

$$[0] = \{\ldots, -3, 0, 3, 6, \ldots\}$$

$$[1] = \{\ldots, -2, 1, 4, \ldots\}$$

$$[2] = \{\ldots, -1, 2, 5, 8, \ldots\}$$

A non-empty subset S of $\mathbb{Z}$ is well-ordered if S contains a least element.

$\mathbb{N} = \{1, 2, 3, \ldots\}$

Principle 2.6 (Principle of Well-Ordering). *Every nonempty subset of the natural numbers is well-ordered.*

The Principle of Well-Ordering is equivalent to the Principle of Mathematical Induction.

Lemma 2.7. *The Principle of Mathematical Induction implies that 1 is the least positive natural number.*

Proof:

$$S = \{n \in \mathbb{N} \mid n \geq 1\} \Rightarrow 1 \in S \quad 1 \geq 1$$

assume $n \in S \quad n \geq 1$

$n+1 \geq 1 \Rightarrow n+1 \in S \therefore$ by induction all natural numbers are in S and $\therefore \geq 1$

Theorem 2.8. *The Principle of Mathematical Induction implies the Principle of Well-Ordering. That is, every nonempty subset of $\mathbb{N}$ contains a least element.*

Theorem 2.9 (Division Algorithm). *Let a and b be integers, with $b > 0$. Then there exist unique integers q and r such that*

$$a = bq + r$$

where $0 \leq r < b$.

Let $a, b \in \mathbb{Z}$

d divides a

- d is a common divisor of a, b if d/a and d/b

$\gcd(a, b) = d$ s.t. all other common divisors of a, b also divide d

- if $\gcd(a, b) = 1 \iff a$ and b are relitivley prime.

Theorem 2.10. *Let a and b be nonzero integers. Then there exist integers r and s such that*

$$\gcd(a, b) = ar + bs.$$

Furthermore, the greatest common divisor of a and b is unique.

Corr) If a, b are relitively pime $\exists\, r, s$ s.t

$1 = ar + bs$

Primes

- P is a prime number if only $1|p$ and $p|p$

Lemma) Let $a, b \in \mathbb{Z}$, P prime If $p|ab$ than either $p|a$ or $p|b$.

Theorem

$a \in \mathbb{Z}$

$a = p_1 \cdots p_1$ for $p_1, \dots, p_n$ prime

Groups

(Informal Definition)

A Group is a set G which is closed under an associative operation s.t. $\exists$ an indentity and inverse

i.e. if $a, b, c \in G$

Associative — operation $= \cdot$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

Identity $e =$ identity is s.t.

$$a \cdot e = e \cdot a = a$$

inverses $a^{-1} =$ inverse of a if

$$a \cdot a^{-1} = a^{-1} \cdot a = e = \text{identity}$$

is closed $a \cdot b \in G$ for all $a, b \in G$

The integers mod n

Recall $a \equiv b \pmod{n}$ iff $a - b = kn$, $k \in \mathbb{Z}$

- Itegers mod n partition $\mathbb{Z}$ into n different eq. classes

- $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$

Operation is addition modulo n

i.e. $\mathbb{Z}_{12}$ = integers mod 12

$[0] = \{ \ldots, -12, 0, 12, 24, \ldots \}$

$\vdots$

$[11] = \{ \ldots, -1, 11, 23, 35, \ldots \}$

- Note that addition and multiplication are defined mod n

$$(a+b) \bmod n = \big((a \bmod n) + (b \bmod n)\big) \bmod (n)$$

$$(a \cdot b) \bmod n = (a \bmod n \cdot b \bmod n) \bmod (n)$$

Ex) $7 + 4 = 1 \pmod 5$, $7 \cdot 3 \equiv 1 \pmod 5$

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Table 3.3: Multiplication table for $\mathbb{Z}_8$

integer mod 8

Not a Group under mult.

Prop Let $\mathbb{Z}_n$ be the set of eq. classes of integers mod n and $a, b, c \in \mathbb{Z}_n$

1) addition and multication are commutive

$$a+b \equiv b+a \pmod{n}$$
$$ab = ba \pmod{n}$$

2) Addition and mult. are associative

3) There are addivite and multiplicitive identites

$$a+0 = a \pmod{n}$$
$$a \cdot 1 = a \pmod{n}$$

4) For every integer a $\exists$ an additive inverse $-a$ s.t.

additive identity

$$a + (-a) = 0 \pmod{n}$$

5) Let $a \neq 0$. Then $\gcd(a,n) = 1$ iff $\exists$ a multiplicitive inverse b for $a \pmod{n}$

i.e. $\exists$ b s.t.

$$ab \equiv 1 \pmod{n}$$

Exist $b, s \in \mathbb{Z}$ s.t.

$$\gcd(a,n) = 1 = ab + ns^{\equiv 0 \bmod n}$$
$$\equiv ab \pmod{n}$$

Corollary 1 $\mathbb{Z}_n$ is a group under addition.

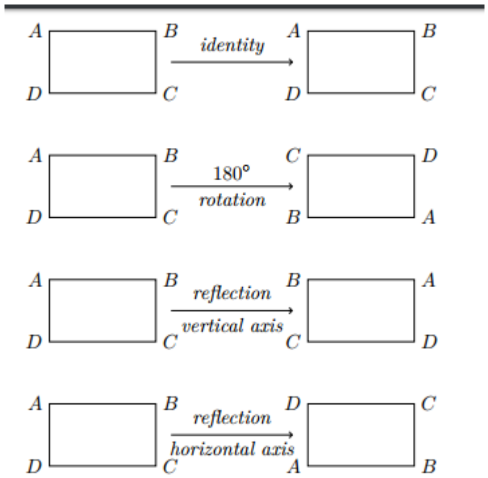


Figure 3.5: Rigid motions of a rectangle

- A symmetry of a geometric figure is a rearrangement of the figure which preserves the shape

- A map from the plane to itself preserving the shape of an object is called a rigid motion

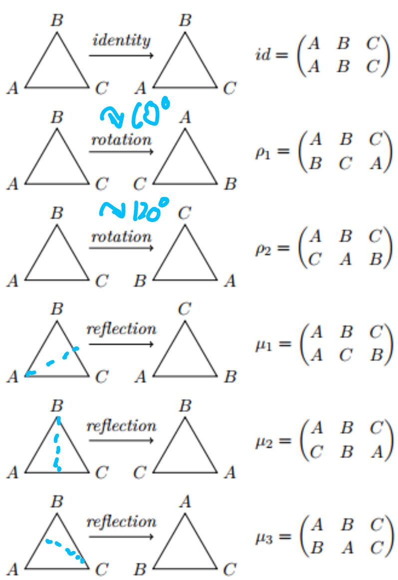


Figure 3.6: Symmetries of a triangle

Recall: a permutation of a set S is a 1-1 and onto map $\pi : S \to S$.

- 3 vertices, this is our set
$\Rightarrow 3! = 6$ permutations

Think about composition of maps (which is associative)

Ex) $\mu_1 \circ \rho_1$, $\mu_1(\rho_1(A)) = \mu_1(B) = C$

$$\mu_1 \rho_1 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} = \mu_2$$

$$\rho_1 \cdot \mu_1 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = \mu_3 \neq \mu_1 \rho_1$$

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

$\therefore$ the symmetries of an equilateral triangle form a group.

Table 3.7: Symmetries of an equilateral triangle

Formal Definition of a Group

A binary operation on a set G is a function $G \times G \to G$ that assigns to each pair $(a,b) \in G \times G$ a unique element $a \cdot b$ or ab or $a \circ b$ or $a + b$.

A group $(G, \circ)$ is a set G with a (closed) binary operation $(a,b) \mapsto a \circ b$ that satisfies the following axioms

- The binary op. is associative, i.e
$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \qquad \forall\, a,b,c \in G$$

- There exists an element $e \in G$ called the identity element s.t $\forall\, a \in G$
$$e \cdot a = a \cdot e = a$$

- For each element $a \in G$ $\exists$ an inverse element in G, a^{-1}, s.t
$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

Note that $a \cdot b \neq b \cdot a$ in general

A group G s.t. $a \cdot b = b \cdot a \quad \forall a, b \in G$ is called an abelian or a commutative group.

Ex) $(\mathbb{Z}_n, +)$ is a group

$$\mathbb{Z}_n = \{0, 1, \dots, n-1\}$$

$\mathbb{Z}_n$ is not a group under mult.

- $U(n) = \{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$ is a group

$$U(8) = \{1, 3, 5, 7\}$$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Table 3.12: Multiplication table for $U(8)$

A matrix Group

$GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \det(A) \neq 0, \; a,b,c,d \in \mathbb{R} \right\}$

$\uparrow$ General linear group, operation is matrix multiplication

Claim: $GL_2(\mathbb{R})$ is a group

- The product of two invertiable matrices is invertable since $\det(AB) = \det(A) \cdot \det(B)$
  or since $(AB)^{-1} = B^{-1}A^{-1}$

- Matrix mult is associative i.e $(AB)\cdot C = A \cdot (BC)$

- Identity is in $GL_2(\mathbb{R})$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$IA = AI = A$$

- Inverses exists $\forall A \in GL_2(\mathbb{R})$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

$\therefore$ $GL_2(\mathbb{R})$ is a group

- Note $GL_2(\mathbb{R})$ is not abelian.

Ex) Let $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$

$J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, $K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$

where $i^2 = -1$

Then

$$Q_8 = \{\pm 1, \pm I, \pm J, \pm K\}$$ is a group.

To check see

$$I^2 = J^2 = K^2 = -1, \quad IJ = K, \quad JK = I, \quad KI = J$$
$$JI = -K, \quad KJ = -I, \quad IK = -J.$$

$$\therefore \quad I^{-1} = -I$$
$$J^{-1} = -J$$
$$K^{-1} = -K$$

Basic properties of Groups

- Groups can be finite or infinite.

· Let G be a group. write $|G|$ = # of elements in G, or the order of G

$$|\mathbb{Z}_5| = 5, \quad |\mathbb{Z}| = \infty$$

<u>Prop</u> | The identity element e of a group G is unique.

<u>Proof</u>: Suppose that $e, \hat{e}$ are identities of G.

$$\Rightarrow \quad eg = ge = g = \hat{e}g = g\hat{e} \quad \forall g \in G$$

$$\therefore \quad eg = \hat{e}g$$, mult. by g^{-1}

$$e g g^{-1} = \tilde{e} g g^{-1} = e \tilde{e} = \tilde{e} e = e = \tilde{e} \quad \blacksquare$$

Prop) If G is a group, $g \in G$, then g^{-1} is unique.

Proof:

Suppose $\tilde{g}, g''$ are both inverses of g

$$g \cdot g'' = g'' \cdot g = e = g \cdot \tilde{g} = \tilde{g} \cdot g$$

$$g g'' = g \tilde{g}$$

$$g^{-1} g g'' = g^{-1} g \tilde{g}$$

$$e g'' = e \tilde{g}$$

$$g'' = \tilde{g}. \quad \blacksquare$$

Prop) G is a group, $a, b \in G$. Then $(ab)^{-1} = b^{-1} a^{-1}$