MATH210: Discrete Mathematics

Mateo Armijo

November 2025

1 Relations

Definition: Let A and B be sets
A relation from A to B is a subset R $R \subseteq A \times B$
Notation: if $(a, b) \in R$ we sometimes write aRb
Definition: R is a relations on A if $R \subseteq A \times A$
Example: $A = \{1, 2, 3\}, B = \{a, b, c, d\}$
$R_1 = \{(1, a), (1, b), (2, b), (3, c)\}$
$R_2 = \{(1, a), (1, b), (1, c)\}$
$R_3 = \{(1, b), (2, d)\}$
are all relations From A to B
Definition: Let R be a relations on A
(i) R is reflexive if $\forall a \in A, (a, a) \in R$
(ii) R is transitive if $(a, b) \in R, (b, c) \in R \implies (a, c) \in R$
(iii) R is symmetric if $(a, b) \in R \implies (b, a) \in R$
(iv) R is antisymmetric if $(a, b) \in R \wedge (b, a) \in R \implies a = b$
Example: Consider $D \subseteq \mathbb{N} \times \mathbb{N}$ where

$$(a, b) \in D \iff^{Defn} a|b \iff b = ak, k \in \mathbb{Z}$$

we can see $(4, 12) \in D, (5, 8) \notin D, (3, 15) \in D$...
Claim: D is reflexive
Proof: Yes are we take $k = 1$ then $a = a \implies a|a \implies (a, a) \in D$
Claim: D is transitive
Proof: Suppose that $(a, b) \in D, (b, c) \in D$

$$\implies b = ak, c = bl, k, l \in \mathbb{Z} \implies c = akl \implies a|c \implies (a, c) \in R$$

Claim: D is not symmetric
Proof: Indeed, $(1, 2) \in D, (2, 1) \notin D$
Claim D is anti symmetric
Proof: Let $a, b \in \mathbb{N}$,
Suppose that $(a, b) \in D, (b, a) \in D$

$$\implies a = bk, b = al \implies b = bkl \implies a(1 - kl) = 0$$

$$\implies k = l = 1$$

So $a = b$
Example: Consider $A = \mathbb{N}$

$$(m, n) \in l \iff (\exists k \in \mathbb{N}_0) : m = n + k$$

Claim: l is reflexive,
Proof: Let $a \in \mathbb{N}$
take $k = 0 \implies a = a + 0$
Claim: l is transitive,
Proof: Given $(a, b) \in l, (b, c) \in l$

$$\implies a + k = b, b + i = c$$

Set $j = i + k$

$$\implies a + i = a + k + i = b + i + c$$

Claim: l is not symmetric
Proof: $(4, 3) \notin l, (3, 4) \in l$
Claim: l is anti symmetric
Proof: Given $(a, b) \in l, (b, a) \in l$

$$\implies a+k = b, b+l = a \implies b+l+k = b \implies l = -k \implies l = k = 0 \implies a = b$$

1.1 Orderings

Definition: Let $X \neq \emptyset$ be a set and R a relation on X
if R is reflexive, transitive, and antisymmetric
then R is called an ordering or a partial ordering on X
We call the pair (X, R) a partially ordered set or an ordered set.
Example: $(\mathbb{N}, D), (\mathbb{N}, l)$ are both ordered sets.
Notation: If (X, R) is an ordered sets, we write $(X, \leq_R)$
Example: Let $S \neq \emptyset$
We can define two orderings on $\mathcal{P}(S)$

$$(A, B) \in I \iff A \subseteq B \text{ We call this the Inclusion ordering}$$

$$(A, B) \in R \iff A \supseteq B \text{ We call this the reverse inclusion ordering}$$

Definition: Let (X, R) be an ordered set, R is total or Linear if $\forall a, b \in X$ either $(a, b) \in R \vee (b, a) \in R$
Example:
(i) $(\mathbb{N}, L)$ is total
(ii) $(\mathbb{N}, D)$ is not total
(iii) $(\mathcal{P}(S), \subseteq)$ is not total unless S has one element
(iv) $(\mathcal{P}(S), \supseteq)$ is not total unless S has one element
Remark: Let $(X, \leq)$ be an ordered set and $Y \subseteq X$, then $Y, \leq)$ is also an ordered

set.
Definition: Let $(X, \leq)$ be an ordered set, suppose $A \subseteq X$
(i) A is bounded above $\iff (\exists u \in X) : (\forall a \in A)(a \leq u)$
(ii) A is bounded below $\iff (\exists u \in X) : (\forall a \in A)(a \geq u)$
(iii) If u is an upper bound of A and $u \in A$ then $u = greastest\{A\}$ or the greatest element of A
(iv) If l is an lower bound of A and $l \in A$ then $l = least\{A\}$ or the greatest element of A
Example: $(\mathbb{N}, D), A = \{5, 12, 16\}$
We see that $5 \cdot 12 \cdot 16$ is an upper bound
Example: $(\mathcal{P}(S), \subseteq)$ suppose $W = \{A, B, C\} \subseteq \mathcal{P}(S)$
We see that A lower bound of W is $\emptyset$ and also $A \cap B \cap C$
similarly, $A \cup B \cup C$ is also an upper bound
Definition: A directed graph is a pair (V, E) of Sets with $E \subseteq V \times V$
V is the set of vertices and E is the set of Edges
if $e \in E$ is an edge from a to b
$e = (a, b)$
So given a relation we can consider the directed graph and given a directed graph we can find a relations
e.g. $R \subseteq A \times A$ we take $V = A, E = R$
Example: (Ordering of functions)
Consider $\mathcal{F}(\mathbb{R}) = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$

$$f \leq g \iff \forall x \in \mathbb{R}, f(x) \leq g(x)$$

We see that is is reflexive since $\forall x, f(x) \leq f(x)$
this is translative because if $\forall x \in \mathbb{R}$ we have $f(x) \leq g(x) \leq h(x) \implies f \leq h$
this is anti symmetric since if $f(x) \leq g(x), g(x) \leq f(x)$ we must have $f(x) = g(x)$
This is not total since $cos(x), sin(x)$
Definition: Let $(X, \leq)$ be an ordered set, $\leq$ is directed if $\forall a, b \in X, \exists c \in X : c \geq a, c \geq b$
Example: We see that $(\mathbb{N}, \leq_D)$ is directed since for any two $m, n \in \mathbb{N}$ we consider $p = mn$ then $p|m, p|n$
Example: Same with the power set and inclusion we can consider $A \cup B$
Example: We consider $(\mathcal{F}(\mathbb{R}), \leq)$. This is directed since given f, g we can consider $h : \mathbb{R} \to \mathbb{R}, h(x) = max\{f(x), g(x)\}$
Example: Let $(X, \leq)$ be an ordered set that is directed.
If $A \subseteq X$ is finite then A is bounded above
Proof: We will preform induction on the number of elements in A.
$A_n = \{a_1, a_2, ..., a_n\}$
Base Case $n = 1$, we see that the upper bound of A_1 is a_1
For $n = 2$ we can use the directedness of X to find $u \in X : u > a_1, u > a_2$

Suppose for some $|A| = m$ we can find an upper bound
Indeed, for $|A_{m+1}| = m + 1$ we write $A_{m+1} = A_m \cup \{a_{m+1}\}$ Using our induc-

tion hypothesis we can find an upper bound of A_m then we use directedness for find an upper bound of the set containing the upper bound of A_m and a_{m+1}
Definition: Let $(X, \leq)$ be an ordered set,
if $(\forall \emptyset \neq A \subseteq X)(\exists l \in A) : (l = least(A))$
then we call X a well ordered set.
e.g. $\mathbb{N}$
Definition: Let $(X, \leq)$ be an ordered set, and $A \subseteq X$
(i) $M \in A$ is maximal if $\forall a \in A$ we have $a \geq M \implies M = a$
(ii) $M \in A$ is minimal if $\forall a \in A$ we have $a \leq M \implies M = a$
Example: $(\mathbb{N}, \leq_D)$

$$m \leq_D n \iff m|n \iff \exists k \in \mathbb{Z} : n = km$$

$A = \{1, 2, 3, 4, 7, 10\}$
Bounded above? Yes take $2 \cdot 3 \cdot 7 \cdot 5$
If does not have a greatest element but has maximal elements,
Yes $3, 4, 7, 10$
Does it have a least element?
Yes 1
Does it have a minimal element?
Yes 1
Definition: Let $(X, \leq)$ be an ordered set.
Suppose $A \subseteq X$
(i) If u is an upper bound of A and $u \leq v$ where v is any upperbound of A then $u := sup(A)$ or the least upper bound of A
(ii)If u is a lower bound of A and $u \geq v$ where v is any lowerbound of A then $u := inf(A)$ or the greatest lower bound of A
Example: Take $(\mathbb{R}, \leq)$ $A = [0, 1)$
We claim that A does not have a greatest element.
Proof: Suppose for contradiction $\exists t \in A : t \geq a \forall a \in A$
Since $t \in A \implies 0 \leq t < 1$
take $\delta = \frac{1+t}{2}$then $t < \delta < 1$ hence $\delta \in A$
Claim: $sup(A) = 1$
Let $x \in A$ then $x < 1$
so 1 is an upper bound
Let v be another upper bound for A, if $v > 1$ we are done
if $v < 1$ consider $\delta = \frac{1+v}{2}$ then $v < \delta < 1$ so $\delta \in A, \delta > v$ so 1 must be the least upper bound.

1.2 Equivalence Relations

Definition: Given a relations R on X
If R is reflexive, transitive,and symmetric then we call R an equivalence relation on X
Notation: $(x, y) \in R \iff x \sim_R y$

Example: Consider the relation on $\mathbb{Q}$,

$$(\mathbb{Q}.\sim_R).R = \{(r,q) \mid r,q \in \mathbb{Q}, r-q \in \mathbb{Z}\}$$

This is non empty since we see that $(\frac{3}{2},\frac{1}{2}) \in R$
Now we will how show that R is an equivalence relation on $\mathbb{Q}$
Proof:
Claim 1: R is reflexive,
Proof: given $r \in \mathbb{Q}, r-r=0 \in \mathbb{Z}$
Claim 2: R is transitive,
Proof: Given $(p,q) \in R, (q,r) \in R$
We know that $p-q \in \mathbb{Z}$ and $q-r \in \mathbb{Z}$ so adding these we get that $p-q+q-r = p-r \in \mathbb{Z}$
Claim 3: R is symmetric
Proof: Given $(p,q) \in R$
we see that $p-q \in \mathbb{Z}$ so multiplying by (-1) we find that $q-p \in \mathbb{Z}$
Example: This will be our running example to motivate our study of probability

$$\Omega := \{(n_k)_{k=1}^{\infty} \mid n_k \in \{0,1\}\}$$

$$(a_k)_k \sim (b_k)_k \iff (\exists N \in \mathbb{N})(\forall k \geq N)(a_k = b_k)$$

We call Ω the coin flip space and we say that this equivalence relation is the tail equivalency,
We claim that $\sim$ is an equivalence relation,
Proof:
Claim 1: Reflexive
Pf: Clearly we just take $N=1$ then $a_k = a_k \forall k \geq 1$
Claim 2: Transitive
Pf: Given $(a_k)_k \sim (b_k)_k, (b_k)_k \sim (c_k)_k$

$$\implies (\exists N_1 \in \mathbb{N}) : (\forall k \geq N_1)(a_k = b_k)$$

$$\implies (\exists N_2 \in \mathbb{N}) : (\forall k \geq N_2)(b_k = c_k)$$

Take $N = max\{N_1, N_2\}$
Then

$$\forall k \geq N, a_k = b_k = c_k$$

Claim 3: Symmetric
pf: Just take the same N,

1.3 Modular Arithmetic

Fix an $n \geq 1$, We define an equivalence relation n on $\mathbb{Z}$

$$a \sim_n b \iff n|a-b$$

We claim this is an equivalence relation. Proof:
Reflexive? $a \sim_n a \iff a - a = nk \iff n|0$
Transitive? Suppose that $a \sim_n b, b \sim_n c$
then

$$a - b = nk, b - c = nl$$

$$\iff a - c = n(k + l)$$

$$\iff n|a - c \implies a \sim_n c$$

Symmetric?

$$a \sim_n b \iff n|a - b \iff a - b = nk, k \in \mathbb{Z}$$

$$\implies -(a - b) = n(-k) \implies b - a = n(-k) \implies b \sim_n a$$

Example: (From $\mathbb{Z}$ to $\mathbb{Q}$),
Consider $X = \mathbb{Z} \times \mathbb{N}$ we define $R \subseteq X \times X$

$$(a, b) \sim (cd) \iff ad = bc$$

We claim that this an equivalence relation
Proof: Reflexive?

$$(a, b) \sim (a, b) \iff ab = ba \iff ab = ab \text{ (Commutativity)}$$

Transitive?
Suppose, $(a, b) \sim (c, d,) \sim (e, f)$
We have $ad = bc, cf = de$

$$afd = bcf = bde \implies d(af - be) = 0 \iff d = 0 \vee (af = be)$$

Since $b \in \mathbb{N}, b \neq 0$
Hence $af = be \implies (a, b) \sim (e, f)$ Symmetric?
$(a, b) \sim (c, d) \iff ad = bc \iff cd = da \iff (c, d) \sim (a, b)$ Definition: Let R be an equivalence relation on a Set X,
Let $x \in X$.
the set $[x]_R$ is the called the equivelence class of x
$[x]_R := \{y \in X \mid y \sim_R x\}$
Facts:
(i) $x \in [x]_R$ (Reflexivity)
(ii) $x \in [y]_R \iff y \in [x]_R$ (Symmetry)
(iii) $[x]_R = [y]_R \iff x \sim_R y$ (Follows from (ii) and transativity)
Proof: (iii)
$\implies$:

$$[x]_R = [y]_R \implies x \in [x]_R = [y]_R \implies x \sim_R y$$

$\impliedby$:
$z \in [x]_R \iff z \sim x$ by transitivity $z \sim y \iff z \in [y]_R$
We call x the representative of the class $[x]_R$,

Example: fix $n = 3$, we had an equivalence relation on $\mathbb{Z}$ $a \sim_3 b \iff 3|a-b$
What does the class of 2 look like? $[2]_3 = \{m \in \mathbb{Z} \mid m \sim_3 2\}$

$$m \in [2]_3 \iff m \sim_3 2 \iff 3|m-2 \iff m = 3k+2$$

Hence $[2]_3 = \{m \in \mathbb{Z} \mid m = 3k+2, k \in \mathbb{Z}\} = \{3k+2 \mid k \in \mathbb{Z}\} = 2 + 3\mathbb{Z}$
What does $[1]_3$ look like?
$1 + 3\mathbb{Z}$
What does $[0]_3$ look like?
$3\mathbb{Z}$
Notice we showed in a homework that $3\mathbb{Z} \cap 3\mathbb{Z}+1 \cap 3\mathbb{Z}+2 \neq \emptyset$
and $\mathbb{Z} = 3\mathbb{Z} \sqcup 3\mathbb{Z}+1 \sqcup 3\mathbb{Z}+2$
Proof:($[1]_3 \cap [2]_3 = \emptyset$)
Suppose for contradiction $\exists m \in [1]_3 \cap [2]_3$
$\implies m \sim 1 \wedge m \sim 2 \implies 1 \sim m \sim 2$(Symmetry)
$\implies 1 \sim 2$ # we can find similarly, they are all pairwise disjoint.
Claim: $\mathbb{Z} \subseteq [0]_3 \sqcup [1]_3 \sqcup [2]_3$
Proof: if $m = 0, 1, 2$ done so suppose that $m > 2$
Consider the set $R = \{m - 3k | k \in \mathbb{Z}\} \cap \mathbb{N}_0$
By the well ordering principle, $\exists l \in R : l = least(R)$
So $0 \leq l = m - 3k \implies 3k = m - l \implies 3|m-l \implies m \sim l$
We claim that $l \in \{0, 1, 2\}$
Pf: Suppose that $l \geq 3 \implies l = 3 + a, a > 0$
$\implies m - 3k = 3 + a \implies m - 3(k+1) = a \iff m - 3j = a \implies a \in R$
But we had that $a < l$ so $a = least(R)$ #
Hence we must have that $m \in [0]_3 \sqcup [1]_3 \sqcup [2]_3$
Proposition: Fix $n \in \mathbb{N}$
Let $\sim_n$ be an equivalence relation on $\mathbb{Z}$
$a \sim_n b \iff n|a-b$
Then,

$$\mathbb{Z} = \bigsqcup_{k=0}^{n-1} [k]_n$$

Proof: fix $n \in \mathbb{N}$
Claim 1: $l \neq k \in \{0, 1, ..., n-1\} \implies [l]_n \cap [k]_n = \emptyset$
Pf:
Suppose for contraction $m \in [k]_n \cap [l]_n$
$\implies m \sim_n l, m \sim_n k$
$\iff l \sim_n m \sim_n k$ (Symmetry)
$\implies l \sim_n k$
$\implies n|l-k \implies l - k = nj$
So $|l-k| < n \implies n > |l-k| = nj \geq n$
Claim 2: Given $m \in \mathbb{Z}, \exists r \in \{0, 1, ..n-1\}$ with $m \in [r]_n$
Proof: If $m \in \{0, 1, ..., n-1\}$ done so suppose that $m \geq n$
Consider $R_m = \{m - nk \mid k \in \mathbb{Z}\} \cap \mathbb{N}_{\not\vdash}$
By well ordering, $\exists r \in R_m : r = least(R_m)$

Then $r \geq 0, r = m - nl, l \in \mathbb{Z}$
Suppose that $r \geq n \implies r = n + a, a > 0$
Then $n + a = m - nl \implies a = m - n(1 + l) \implies a \sim m \implies a \in R_m, a \leq r$
so r is not the least element.
Proposition: Let $\sim_R$ be an equivalence relation on X
for any $[a], [b]$ either $[a] = [b]$ or $[a] \cap [b] = \emptyset$
We can also write $X = \bigsqcup_{i \in I} [x_i]$
Claim: $(\exists x \in [a] \cap [b]) \implies [a] = [b]$
Proof: Suppose for contradiction, $(\exists y \in [a], y \notin [b])$
then $x \sim y \implies y \sim x \sim b \implies y \sim b \implies y \in [b]$
Definition: Let A be a set, a partition of A is a family of pairwise disjoint subsets $\{A_i\}_{i \in I}$ such that $A = \bigsqcup_{i \in I} A_i$
Example: $\mathbb{N} = \mathbb{E} \cup \mathbb{O} = [0]_2 \sqcup [1]_2$
Example: $\mathbb{N} = \bigsqcup_{n \in \mathbb{N}} [n]$
Challenge: Write $\mathbb{N}$ as the disjoint union of infinite sets.
$\mathbb{N} = \bigsqcup_{n=1}^{\infty} N_k, N_k$ infinite
Proposition: Given a partition $\bigsqcup_{i \in I} X_i = X$ we can define an equivalence relation on X
$x, y \in X, x \sim y \iff (\exists i \in I) : (x, y \in X_i)$
Definition: Let R be an equivalence relation on X
(i) $x \in X, [x]_R = \{y \in X \mid y \sim_R x\}$
(ii) $X/R = \{[x]_R \mid x \in X\}$
Example: $\mathbb{Z}/\sim_n = \{[m] \mid m \in \mathbb{Z}\}$
this has n elements and each element is a class. Point being we wish to do operation on this set.
We want to make an algebra recall, we have $(\mathbb{N}, \times, +)$ and with $(\mathbb{Z}, \times, +, -)$
We claim that on $(\mathbb{Z}/\sim_n)$ has $[a]_n + [b]_n = [a + b]_n$ is a well defined.
Proof: Suppose we have $[a']_n = [a]_n$ and $[b']_n = [b]_n$
$[a']_n = [a]_n \iff a \sim a' \iff n | a - a' \iff kn = a - a'$
similarly we have $ln = b - b' \implies b | a + b - a' - b' \iff a + b \sim a' + b' \iff [a + b] = [a' + b']$

1.3.1 Forming the Rationals

Consider the Set $X = \mathbb{Z} \times \mathbb{Z}^*, \mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$
Let Q be an equivelence relation on X.

$$(a, b) \sim (c, d) \iff ad = bc$$

We consider $X/Q := \{[(a, b)] \mid a, b \in \mathbb{Z}, b \neq 0\}$
Claim 1: $[(a, b)] = \{(an, bn) \mid n \in \mathbb{Z}\}$
e.g. $[(4, 6)] = \{(2n, 3n) \mid n \in \mathbb{Z}^*\}$
Proof: Certainly, $(2n, 3n) \sim (4, 6)$,
Now Suppose that $(x_1, x_2) \in [(4, 6)] \implies (x_1, x_2) \sim (4, 6)$
$\implies 6a - 4b \implies 3a = 2b \implies 3a$ is even

So we write $a = 2n$, now we have $3a = 2n = 2b \implies n = b$
So $(a, b) \sim (2n, 3n)$
Given $a, b \in \mathbb{Z}, b \neq 0$ we write $a = ka', b = kb'$ where a' and b' have no common factor.
Claim: $([a, b]) = \{(na', nb') \mid n \in \mathbb{Z}, n \neq 0\}$
Now we can define operations on $\mathbb{Q} := X/Q$
We will verify that $(\mathbb{Q}, +)$ is well defined.
Proof: Suppose $[(a, b)] = [(a', b')], [(c, d)] = [(c', d')]$

$$[(a, b)] = [(a', b')] \iff (a, b) \sim (a', b') \implies ab' = a'b$$

Similarly,

$$cd' = c'd$$

So we consider

$$\begin{aligned} & bd(a'd') + bd(c'b') = b'd'(ad) + b'd'(cb) \\ \iff & a'bdd' + c'b'bd = a'd'bd + bdb'c' \\ \iff & a'bdd' + b'c'db = a'd'bd + bdb'c' \\ \iff & b'd'(ad + bc) = bd(a'd' + b'c') \end{aligned}$$

Notice $(\mathbb{Q}, +), + : \mathbb{Q} \to \mathbb{Q}$
we have:
(i) $a + (b + c) = (a + b) = c$ (Associativity)
(ii) $a + 0 = a = 0 + a$ (Additive Identity)
(iii) $(\forall q \in \mathbb{Q})(\exists! q^{-1} \in \mathbb{Q}) : q + q^{-1} = 0$ (Additive inverses)
(iv) $a + b = b + a$ (Commutativity) This are the requirements for an abelian group.
Now we consider $\cdot : \mathbb{Q} \to \mathbb{Q}, [(a, b)] \cdot [(c, d)] = [(ac, bd)]$
It can be proved that this is well defined,
we also have:
(1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$(Associativity)
(2) $a \cdot 1 = a = 1 \cdot a$ (Multiplicative identity)
(3) $a \cdot b = b \cdot a$ (Commutativity)
(4) $(\forall q \in \mathbb{Q})(\exists! q^{-1} \in \mathbb{Q}) : qq^{-1} = 1$
Proof: (4)
Given $q = [(a, b)] \neq 0$,
$\implies a \neq 0$ Choose $q^{-1} = [(b, a)]$
Then we have $qq^{-1} = [(ab, ab)] = 1$
With this all said we define $[(a, b)] = \frac{a}{b}$

1.4 Functions:

Definition: Let $X, Y \neq \emptyset$, a function is a relation from X to Y, $f \subseteq X \times Y$ such that

$$(\forall x \in X)(\exists! y \in Y)((x, y) \in f)$$

We call $X = Dom(f), Y = CoDom(f)$
we write $f : X \to Y$ to denote a function from X to Y
also if $(x, y) \in f$ we write $f(x) = y$ because the y is unique,
Definition: If $f : X \to Y$ then
$Im(f) = \{f(x) \mid x \in X\} \subseteq Y$
Example: $f = \{(x, y) \mid x^2 + y^2 = 1\}$
f is clearly a relation from X to Y but is f a function?
Solution:
No Since $x = 0 \implies (0, 1), (0, -1) \in f$
so it violates the uniqueness.
$g = \{(x, y) \mid x \in X, y, \in Y, y \geq 0, x^2 + y^2 = 1\}$ Now it is a function.
$h = \{(x, y) \mid x \in [-1, 1], y \in [0, 1], x^2 + y^2 = 1\}$
We see that $g \neq h$ since the need to have to be identical as sets and that is not true.
Example: Consider $f : \mathbb{Z}/\sim_n \to \mathbb{Z}$.
$f([k]_n) = k$ is not well defined,
$f([0]_n) = 0, f([0]_n = [n]_n) = n$
When defining a function you need your choices to be well defined
Example: $f : \mathbb{Z}/\sim_6 \to \mathbb{Z}/\sim_3$
We claim that f is well defined,
Proof: If $[a]_6 = [a']_6$ then

$$a \sim_6 a \implies 6|a - a' \implies 3|a - a'$$

Hence, $[a]_3 = [a']_3$
Therefore, $f([a]_6) = f([a']_6)$
Definition: Let $f : X \to Y$,
Suppose $A \subseteq X, B \subseteq Y$
(i) The Image of A under f is
$f(A) := \{f(a) \mid a \in A\}$
(ii) The PreImage of B under f is
$f^{-1}(B) := \{x \in X \mid f(x) \in B\} \subseteq X$
Notice $Im(f) = f(X)$ and $f^{-1}(B)$ can be empty,
Example: $f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$ (i) $A = [-1, 4], f(A)$?
(ii) $B = \{-1, 2\}, f^{-1}(B)$?
(iii) $f^{-1}((-\infty, 0))$? Solution: (i)$f(A) = \{f(a) \mid a \in A\}$
$= \{a^2 \mid a \in [-1, 4]\} = \{a^2 \mid -1 \leq a \leq 4|\}$
so if

$$0 \leq a \leq 4 \iff 0 \leq a^2 \leq 16$$

if

$$-1 \leq a \leq 0 \iff 1 \geq a^2 \geq 0$$

So $0 \leq a^2 \leq 16$
(ii) $f^{-1}(B) = \{1, -1, \sqrt{2}, -\sqrt{2}\}$

(iii) $\emptyset$
Example:
Consdier $\Omega = \{(a_k)_k \mid a_k \in \{0,1\}\}$
if $F \subseteq \mathbb{N}$, is finite, consider $\sigma_F : \Omega \to \Omega : \sigma_F((a_k)_k) = (b_k)_k$, $b_k = \begin{cases} a_k & k \notin F, \\ 1 - a_k & k \in F. \end{cases}$
This just switches the terms of the sequence $(a_k)_k$ to the opposite if their index is in F
and Recall our equivalence relations on Ω

$$(a_k)_k \sim (b_k)_k \iff (\exists N \in \mathbb{N})(\forall k \geq N)(a_k = b_k)$$

We claim that $[\omega] = \{\sigma_F(\omega) \mid F \subseteq \mathbb{N} \text{ finite}\}$
Proof:
Claim 1: $[\omega] \subseteq \{\sigma_F(\omega) \mid F \subseteq \mathbb{N}\}$
Proof:

$$(x_k)_k \in [\omega] \iff (\exists N \in \mathbb{N}) : (\forall k \geq N)(x_k = \omega_k)$$

Consider the finite set $\mathcal{F} = \{n \mid n < N\}$
Find $F \subseteq \mathcal{F} : (x_k) = \sigma_F(\omega)$
hence, $(x_k) \in \{\sigma_F(\omega) \mid F \subseteq \mathbb{N} \text{ finite}\}$
Claim 2: $\{\sigma_F(\omega) \mid F \subseteq \mathbb{N} \text{ finite}\} \subseteq [\omega]$
Proof:

$$(x_k)_k \in \{\sigma_F(\omega) \mid F \subseteq \mathbb{N} \text{ finite}\} \iff (\exists F \subseteq \mathbb{N} \text{ finite}) : (\sigma_F(\omega) = (x_k)_k$$

Since F is finite we find $N = max(F)$
then $\forall k > M, x_k = \omega_k$

$$\implies (x_k)_k \sim \omega \iff (x_k)_k \in [\omega]$$

Theorem:(Well Definite theorem)
Let $X, Y \neq \emptyset$ be sets,
and $\sim$ be an equivalence relations on X
and $f : X \to Y$ be any function
If $x \sim x' \implies f(x) = f(x')$
Then $\exists! g : X/\sim \to Y$
We call $X/\sim$ the quotient space,
Proof: Definite $g([x]_\sim) = f(x)$ We claim that g is a function(well defined)
Suppose $(\exists [x] = [x'])$
so $x \sim x'$ By assumption $f(x) = f(x')$
Hence $g([x]) = g([x'])$
So we take $\pi : X/\sim \to Y$
and we find that $f \circ \pi = g$
so $g : X/\sim \to Y$ exists.
Uniqueness Suppose we have $h : X/\sim \to Y$, $g([x]) = f(x)$
By definition we have $h([x]) = g([x])$

Example: $f : \mathbb{Z} \to \mathbb{Z}/\sim_6$: $f(m) = [2m]_6$, Suppose that $m \sim_3 n$,

$$3|m-n \iff m-n = 3k \iff 2m-2n = 6k \iff 6|2m-2n \iff [2m]_6 = [2n]_6$$

By Theorem $\exists! f^* : \mathbb{Z}/\sim_3 \to \mathbb{Z}/\sim_6$
Example: $p(x) = \frac{1}{1+x^2}$ give a suitable domain and co-domain, whats the image of f over its domain?
Solution: We can take $p : \mathbb{R} \to \mathbb{R}$. we claim that $Im(f) = (0, 1]$,
$1 + x^2 \geq 1 \implies \frac{1}{1+x^2} \leq 1$ and $0 < \frac{1}{1+x^2}$ So $Im(f) \subseteq (0, 1]$
Now we claim that $(0, 1] \subseteq Im(f)$
let $t \in (0, 1]$

$$p(x) = t \iff \frac{1}{1+x^2} = t \iff x^2+1 = \frac{1}{t} \iff x^2 = \frac{1}{t}-1 \iff x = \sqrt{\frac{1}{t}-1}$$

Proposition: If $f : X \to Y$ is a map, $A \subseteq X, B \subseteq Y$
(i) $f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i)$
(ii) $f(\bigcap_{i\in I} A_i) \subseteq \bigcap_{i\in I}(f(A_i))$
(iii) $f(A^c) \neq f(A)^c$ generally,
Proof:
(i)

$$y \in f(\bigcup_{i\in I} A_i) \iff (\exists x \in \bigcup_{i\in I} A_i) : (f(x) = y) \iff (\exists i \in I)(\exists x \in A_i) : (f(x) = y)$$

$$\iff (\exists i \in I) : (y \in f(A_i)) \iff y \in \bigcup_{i\in I} f(A_i)$$

(ii)

$$y \in f(\bigcap_{i\in I} A_i) \implies (\exists x \in A_i) : (\forall i \in I)(y = f(x)) \iff y \in \bigcap_{i\in I} f(A_i)$$

Proposition:
If $f : X \to Y$ is a map, $A \subseteq X, B \subseteq Y$
(i) $f^{-1}(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f^{-1}(A_i)$
(ii) $f^{-1}(\bigcap_{i\in I} A_i) = \bigcap_{i\in I}(f^{-1}(A_i))$
(iii) $f^{-1}(A^c) = f^{-1}(A)^c$
Proof: (i)
$x \in f^{-1}(\bigcup_{i\in I} A_i)$
$\iff (\exists y \in \bigcup_{i\in I} B_i) : (f(x) = y)$
$\iff (\exists i \in I)(\exists y \in B_i) : (f(x) = y)$
$\iff (\exists i \in I) : (x \in f^{-1}(B_i))$
$\iff x \in \bigcup_{i\in I} f^{-1}(B_i)$
(ii)
$x \in f^{-1}(\bigcap_{i\in I} A_i)$
$\iff (\forall i \in I)(\exists y \in B_i) : (f(x) = y)$
$\iff (\forall i \in I)(x \in f^{-1}(B_i))$

$\iff x \in \bigcap_{i\in I} f^{-1}(B_i)$
(iii)
$x \in f^{-1}(B^c)$
$\iff (\exists y \in B^c) : (f(x) = y)$
$\iff (\exists y \in B) : (f(x) \neq y)$
$\iff (x \notin f^{-1}(B))$
$\iff x \in (f^{-1}(B))^c$

Definition: A function $f : X \to Y$ A function $f : X \to Y$ is surjective if

$$(\forall y \in Y)(\exists x \in X) : (f(x) = y)$$

equivalently, $Im(f) = Y$
or $(\forall y \in Y)(f^{-1}(\{y\}) \neq \emptyset)$
We call $f^{-1}(\{y\})$ the fiber of f over y,
we have the fibers are disjoint by uniqueness of functions. So we can partition $X = \bigsqcup_{y\in Y} f^{-1}(\{y\})$
Example: $\pi : \mathbb{Z} \to \mathbb{Z}/5$
$\pi^{-1}([1]_5) = 1 + 5\mathbb{Z}$ $\pi^{-1}([2]_5) = 2 + 5\mathbb{Z}$ $\pi^{-1}([3]_5) = 3 + 5\mathbb{Z}$ $\pi^{-1}([4]_5) = 4 + 5\mathbb{Z}$
$\pi^{-1}([0]_5) = 5\mathbb{Z}$ Example: $\lceil (x) \rceil : \mathbb{R} \to \mathbb{Z}$
we have that $f^{-1}(\{n\}) = (n-1, n]$
and $\mathbb{R} = \bigsqcup_{n\in\mathbb{Z}} f^{-1}(\{n\})$
Proposition: Let $f : X \to Y$ be a function,
$A \subseteq X, B \subseteq Y$,
(i) $A \subseteq f^{-1}(f(A))$
(ii) $f(f^{-1}(B)) \subseteq B$
Proof:
(i) Let $a \in A$

$$\implies f(a) \in f(A) \implies a \in f^{-1}(f(A))$$

(ii)
Let $y \in f^{-1}(f(B))$

$$\implies y \in f(x), x \in f^{-1}(B) \implies y \in B$$

The Algebra of Functions:
Fix $S \neq \emptyset$,
(i) $id_S : S \to S, id_S(x) = x$
(ii) Let $A \in S, \mathbb{1}_A := \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$
if $A = \{a\}$
we says that $\mathbb{1}_{\{a\}} = \delta_a$
Example: Consider $\mathbb{1}_A, \mathbb{1}_B : S \to \mathbb{R}$
$\mathbb{1}_A = \mathbb{1}_B \iff A = B$
Proof: We see that $\mathbb{1}_A = \mathbb{1}_B \iff {}_A = \mathbb{1}_B, (\forall x \in \Omega)$
So if $x \in A \iff \mathbb{1}_A = 1$
$\iff 1 = \mathbb{1} \iff x \in B$

Hence $A = B$
Definition: Fix $S \neq \emptyset$, Let $\mathcal{F}(S, \mathbb{R}) = \{f \mid f : S \to \mathbb{R}\}$
for $f, g \in \mathcal{F}(S, \mathbb{R}), t \in \mathbb{R}$, Define

$$(i)(f \pm g)(x) = f(x) \pm g(x)$$

$$(ii)(tf)(x) = tf(x)$$

$$(iii)(fg)(x) = f(x)g(x)$$

If $g(x) \neq 0, \forall x \in S$

$$(iv)\frac{1}{g}(x) = \frac{1}{g(x)}$$

We says that $\mathbb{1}_\emptyset = 0$
and $\mathbb{1}_S = 1$
Example: $\mathbb{1}_A \cdot \mathbb{1}_B = \mathbb{1}_{A \cap B}$
Proof: Let $x \in S$
if $S \in A \cap B$
then $\mathbb{1}_{A \cap B}(x) = 1$
and $\mathbb{1}_A \cdot \mathbb{1}_B = 1$
Without loss of generality, $x \in A, x \notin B$
then $\mathbb{1}_{A \cap B}(x) = 0$
and $\mathbb{1}_A \cdot \mathbb{1}_B = 0$
We notice also $\mathbb{1}_{A \cup B} = \mathbb{1}_A + \mathbb{1}_B - \mathbb{1}_{A \cap B}$
Definition: Let $f \in \mathcal{F}(S, \mathbb{R})$
if $Im(f)$ is finite then we call f simple.
Example: if $im(f) = \{a_1, a_2, .., a_n\}$
we can express $f = \sum_{k=1}^{n} a_k \mathbb{1}_{f^{-1}(\{a_k\})}$
Composition of Functions:
Definition: Let $f : X \to Y, g : Y \to Z$
We define $g \circ f : X \to Z, g(f(x))$
Note that $im(f) \subseteq Dom(g)$

1.5 A Glimpse of Probability

Throughout, Let Ω be a finite set, we can refer to Ω as the sample space.
Example: Consider $\Omega := \{(x, y) \mid 1 \leq x \leq 6, 1 \leq y \leq 6\} = \{(1,1), (1,2), ..., (1,6), (2,1), ..., (6,6)\}$
Notice that this can be interpreted as the set of all possible ways to roll two distinguishable dice. $|\Omega| = 36$ and the "Probability" of getting an outcome is $\frac{1}{36}$ for any combinations. Definition:
If $P : \Omega \to [0, 1] : \sum_{x \in \Omega} P(x) = 1$ then we call P a probability function on Ω
In our above example we see that $P(i, j) = \frac{1}{36}$ we call this a uniform probability.
Given a probability function we wish to talk about a probability measure. i.e. we wish the find the probability of a subset of events rather than a single one.
In the dice example consider $E = \{(i, j) \in \Omega \mid i + j = 5\}$ what is the likelihood of $i + j = 5$? In this example we can just list them our and see we have 4 elements

in E and hence $\frac{4}{36}$
Definition:
If $\mu : \mathcal{P}(\Omega) \to [0,1]$ meaning $(\forall E \subseteq \Omega)(E \mapsto \mu(E) \in [0,1]$ with the following properties:
(i) $\mu(\emptyset) = 0$
(ii) $\mu(\Omega) = 1$
(iii) if $\{E_i\}_{i \in I}$ is a pairwise disjoint family of subsets of Ω
then $\mu(\bigsqcup_{i \in I} E_i) = \sum_{i \in I} \mu(E_i)$
Then we call μ a probability measure on Ω
So given a probability functions $P : \Omega \to [0,1]$ we get $\mu_P : \mathcal{P}(\Omega) \to [0,1]$
a probability measure with $\mu_P(E) = \sum_{w \in E} P(w)$
In the above example where $E = \{(i,j) \in \Omega \mid i + j = 5\}$, $\mu_P(E) = \frac{1}{9}$
Proposition: $\mu(E^c) = 1 - \mu(E)$
Proof: $E^c \cap E = \emptyset, E^c \cup E = \Omega \implies E^c \sqcup E = \Omega$
Hence,

$$1 = \mu(\Omega) = \mu(E^c \sqcup E) = \mu(E^c) + \mu(E) \iff \mu(E^c) = 1 - \mu(E)$$