CS1231S Discrete Structures

$\forall \cdot \exists \cdot \subseteq \cdot \in$

IMPORTANT SETS

$\mathbb{N}$: Set of all natural number $\{1, 2, 3, \ldots\}$, excludes zero.

$\mathbb{Z}$: Set of all integers

$\mathbb{Q}$: Set of all rational numbers

$\mathbb{R}$: Set of all real numbers

|x|

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \end{cases}$$

INTEGER PROPERTIES

$\forall x, y, z \in \mathbb{Z}$,

Closure: Integer closed under addition and multiplication.

$x+y \in \mathbb{Z}$, $xy \in \mathbb{Z}$.

Commutativity

Distributivity

Associativity

Trichotomy: Exactly one is true — $x=y$, or $x>y$, or $x<y$.

EVEN OR ODD

For any integer n,

n is even $\iff \exists$ an integer k such that $\boxed{n=2k}$.

n is odd $\iff \exists$ an integer k such that $\boxed{n=2k+1}$

DIVISIBILITY

$n, d \in \mathbb{Z}$, $d \neq 0$. Then:

$\boxed{d \mid n \iff \exists k \in \mathbb{Z} \text{ s.t. } n = dk.}$

↳ d divides n.

i.e. n is divisible by d iff n equals d times some integer.

RATIONAL NUMBERS

A real number r is rational iff it can be expressed as a quotient of two integers with a nonzero denominator.

$\boxed{r \text{ is rational} \iff \exists a, b \in \mathbb{Z} \text{ s.t. } r = \frac{a}{b} \text{ and } b \neq 0.}$

Irrational: Real number t is not rational.

PROOF

Prove that $P \rightarrow Q$

start of proof. (P) — end of proof (Q)

Definition of P → … → Definition of Q.

Types of Proof

- Direct Proof
- Proof by Construction
- Disproof by Counterexample
- Proof by Exhaustion
- Proof by Contradiction

Prepared by: Joshua Chew Jian Xiang @joshuaaaah

LOGICAL CONNECTIVES

$\sim$	Not/Negation	Performed first
$\wedge$	And/conjunction	Coequal in order of operation.
$\vee$	or/disjunction	
$\oplus$	exclusive-or $p \oplus q \equiv (p \vee q) \wedge \sim(p \wedge q)$	
$\rightarrow$	implies	Performed last. Coequal in order of operation.
$\Leftrightarrow$	biconditional	

VALID ARGUMENT FORMS

Modus Ponens.	If p then q. p. $\therefore q$.
Modus Tollens.	If p then q. $\sim q$. $\therefore \sim p$.
Generalization.	p. $\therefore p \vee q$.
Specialization.	$p \wedge q$. $\therefore p$.
Elimination.	$p \vee q$. $\sim q$. $\therefore p$.
Transitivity	$p \rightarrow q$. $q \rightarrow r$. $\therefore p \rightarrow r$.
Division into Cases.	$p \vee q$. $p \rightarrow r$. $q \rightarrow r$. $\therefore r$.

Also:

Conjunction: p. q. $\therefore p \wedge q$.

Contradiction Rule: $\sim p \rightarrow$ false. $\therefore p$.

LOGICAL EQUIVALENCES

Commutative Laws "Appy laws"	$p \wedge q \equiv q \wedge p$ $p \vee q \equiv q \vee p$
Associative Laws "jumpy brackets"	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ $(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive Laws "expansion"	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity Laws	$p \wedge \text{true} \equiv p$ $p \vee \text{false} \equiv p$
Negation Laws	$p \vee \sim p \equiv \text{true}$ $p \wedge \sim p \equiv \text{false}$
Double negative law	$\sim(\sim p) \equiv p$
Idempotent Laws	$p \wedge p \equiv p$ $p \vee p \equiv p$
Universal Bound Laws	$p \vee \text{true} \equiv \text{true}$ $p \wedge \text{false} \equiv \text{false}$
De Morgan's Laws "spread the negativity"	$\sim(p \wedge q) \equiv \sim p \vee \sim q$ $\sim(p \vee q) \equiv \sim p \wedge \sim q$
Absorption Laws	$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$
Negation of true and false	$\sim \text{true} \equiv \text{false}$ $\sim \text{false} \equiv \text{true}$
Implication Laws	$p \rightarrow q \equiv \sim p \vee q$

FALLACIES

Converse Error	$p \rightarrow q$. q. $\therefore p$.
Inverse Error	$p \rightarrow q$. $\sim p$. $\therefore \sim q$.

Valid argument but false premise & false conclusion.

Invalid argument with true premises & true conclusion.

PREDICATES

$Q(x,y) =$ " x is a student at y ".

$P(x) =$ " x is a student at Cinnamon College". — predicate

↳ x has domain D.

Truth set of $P(x)$ is $\{x \in D \mid P(x)\}$

QUANTIFIED STATEMENTS

$\forall$ for all/universal Quantifier

$\exists$ there exists/existential quantifier

$\exists!$ there exists a unique/there is one and only one

Universal Statement	$\forall x \in D\, (Q(x))$
Existential Statement	$\exists x \in D$ such that $Q(x)$
Universal Conditional Statement	$\forall x\, (P(x) \rightarrow Q(x))$

Vacuously true iff $P(x)$ is false for every x in D.

$\boxed{\sim(\forall x \in D, Q(x)) \equiv \exists x \in D \text{ such that } \sim Q(x)}$

$\boxed{\sim(\exists x \in D \text{ such that } Q(x)) \equiv \forall x \in D, \sim Q(x)}$

$\boxed{\sim(\forall x, P(x) \rightarrow Q(x)) \equiv \exists x \text{ such that } P(x) \wedge \sim Q(x)}$

Rule of Universal Instantiation: If some property is true of everything in the set, then it is true for any particular thing in the set.

CONDITIONAL STATEMENTS

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

$p \rightarrow q$ is false only if the conclusion q is false.

Vacuously true: $p \rightarrow q$ is true if the hypothesis p is false.

"If Joshua is a girl, then Joshua can fly."

p — hypothesis/antecedent

q — conclusion/consequent

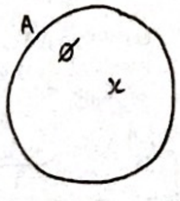
$p \rightarrow q$ Statement	$\equiv \sim q \rightarrow \sim p$ Contrapositive
$q \rightarrow p$ Converse	$\equiv \sim p \rightarrow \sim q$ Inverse

NECESSARY/SUFFICIENT

Statement	Statement form
p if q $\equiv$ if q then p	$q \rightarrow p$
p only if q $\equiv$ if p then q	$p \rightarrow q$
p if, and only if, q $\equiv$ p iff q.	$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

r is a sufficient condition for s	if r then s.
r is a necessary condition for s	if not r then not s $\equiv$ if s then r
r is a necessary and sufficient condition for s	r, if and only if s.

SET NOTATION



A set is an unordered collection of objects

$x \in A$: Object x is in the set A.

$x \notin A$: Object x is not in the set A.

Proving that an object is an element of a set:

If $A = \{x \mid P(x)\}$, to prove that $a \in A$, we need to show that $P(a)$ is true.

$\mathcal{U}$: the universal set, containing all elements under discussion.

$\emptyset$: the empty set.

SUBSETS

Set A is a subset of set B; if every element of A is also an element of B.

$\boxed{A \subseteq B \equiv \forall x (x \in A \rightarrow x \in B)}$

A is not a subset of B:

$\boxed{A \nsubseteq B \equiv \exists x (x \in A \wedge x \notin B) \equiv \exists x \in A (x \notin B)}$

Important Notes:

- For any set A, $\varnothing \subseteq A$ and $A \subseteq A$.

When $A = \{x \mid p(x)\}$ and $B = \{x \mid q(x)\}$,

$\boxed{A \subseteq B \equiv \forall x,\ p(x) \rightarrow q(x)}$

If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

EQUAL SETS

Two sets A and B are equal if they contain the same elements.

$\boxed{(A=B) \equiv (A \subseteq B) \wedge (B \subseteq A) \equiv \forall x\ (x \in A \Leftrightarrow x \in B)}$

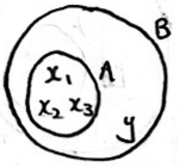
PROPER SUBSETS

A subset A of B is proper if $A \neq B$.

A is a proper subset of B:

$A \subsetneq B$

$\Leftrightarrow (\forall x \in A, x \in B) \wedge (\exists y \in B, y \notin A)$



ELEMENT METHOD

To show that $\boxed{A \subseteq B}$ we must show that $\boxed{x \in A \Rightarrow x \in B}$.

To show that $\boxed{A = B}$, we must show:

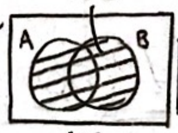
1. $\boxed{x \in A \Rightarrow x \in B}$
2. $\boxed{y \in B \Rightarrow y \in A}$

OR, show: $\boxed{x \in A \Leftrightarrow x \in B}$.

SET OPERATIONS

Union of A and B:

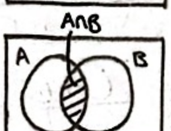
$\boxed{A \cup B = \{x \in \mathcal{U} \mid x \in A \vee x \in B\}}$



Intersection of A and B:

$\boxed{A \cap B = \{x \in \mathcal{U} \mid x \in A \wedge x \in B\}}$

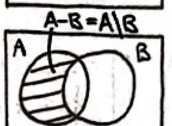
"Strictly both A and B"



Complement of B in A:

$\boxed{A - B = A \setminus B = \{x \in A \mid x \notin B\}}$

"A but not B"



Complement of B:

$\boxed{\overline{B} = \mathcal{U} - B}$

$\boxed{\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n}$

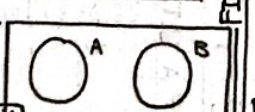
(For 3 or more sets)

$\boxed{\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap \cdots A_n}$

DISJOINT SETS

Two sets A and B are disjoint if:

$\boxed{A \cap B = \varnothing}$



For disjoint finite sets, $\boxed{|A \cup B| = |A| + |B|}$

Let $\mathcal{B}$ be a collection of sets.

The sets in $\mathcal{B}$ are pairwise disjoint iff $\boxed{\forall A, B \in \mathcal{B} \text{ with } A \neq B, \text{ we have } A \cap B = \varnothing.}$

For pairwise disjoint finite sets $A_1, A_2, \ldots, A_n$, $\boxed{\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| = |A_1| + |A_2| + \cdots + |A_n|}$

SET IDENTITIES

Commutative Laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative Laws	$(A \cup B) \cup C = A \cup (B \cup C)$	
	$(A \cap B) \cap C = A \cap (B \cap C)$	
Distributive Laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	
	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	
Identity Laws	$A \cup \varnothing = A$	$A \cap \mathcal{U} = A$
Idempotent Laws	$A \cup A = A$	$A \cap A = A$
Complement Laws	$A \cup \overline{A} = \mathcal{U}$	$A \cap \overline{A} = \varnothing$
Universal Bound Laws	$A \cup \mathcal{U} = \mathcal{U}$	$A \cap \varnothing = \varnothing$
Double Complement Law	$\overline{(\overline{A})} = A$	
De Morgan's Laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	
	$\overline{A \cap B} = \overline{A} \cup \overline{B}$	
Absorption Laws	$A \cup (A \cap B) = A$	
	$A \cap (A \cup B) = A$	
Set Difference Law	$A - B = A \cap \overline{B}$	
Complements of Universal and Null Set	$\overline{\mathcal{U}} = \varnothing$	$\overline{\varnothing} = \mathcal{U}$.

CARTESIAN PRODUCTS

Cartesian Product of A and B,

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

(a,b) → ordered pairs

$(a,b) \neq (b,a)$ unless $a = b$.

$A^n = \underbrace{A \times A \times \cdots \times A}_{n}$

Cartesian Product of $A_1, A_2, \ldots, A_n$,

$\boxed{A_1 \times A_2 \times \cdots \times A_n := \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}}$

$(a_1, a_2, \ldots, a_n)$ → n-tuples

POWER SETS

Power Set of A, is the set of all the subsets of A.

$\boxed{\mathcal{P}(A) = \{X \mid X \subseteq A\}}$

Important Notes:

$\mathcal{P}(\{1,2\}) = \{\varnothing, \{1\}, \{2\}, \{1,2\}\}$

$\mathcal{P}(\varnothing) = \{\varnothing\}$

PARTITIONS

A partition of A is an unordered collection of pairwise disjoint, non-empty subsets of A whose union is A.

P is a partition of A iff:

- $P \subseteq \mathcal{P}(A)$; "subsets"
- $\varnothing \notin P$; "non-empty"
- Distinct elements of P are pairwise disjoint, ie. $\forall X, Y \in P$ with $X \neq Y$, we have $X \cap Y = \varnothing$
- $\bigcup_{X \in P} X = A$ "union is A"

Note that P is not unique.

If A is non-empty, then $\{A\}$ is a partition of A.

Lemma: $\{A \cap B, A - B, B - A\}$ is a collection of pairwise disjoint subsets of $A \cup B$ whose union is $A \cup B$.

FINITE SETS

A set is finite if it contains only finitely many distinct elements.

A set is infinite if it contains infinitely many distinct elements.

S is a finite set:

$\boxed{|S| = \text{Number of distinct elements in } S.}$

For finite sets, not necessarily disjoint:

$\boxed{|A \cup B| = |A| + |B| - |A \cap B|}$

FUNCTIONS

A function f from a set A to a set B is a rule that assigns to each element $a \in A$ a unique element $f(a) \in B$

$\boxed{f: A \to B;\ a \mapsto f(a)}$ A → domain of f, B → codomain of f.

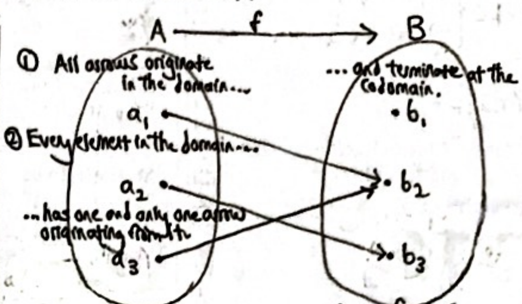
$\boxed{f: \mathbb{R} \to \mathbb{R};\ f(a) = a^2 + a + 1}$

A function $f: A \to B$ is well-defined iff:

① f defines a unique $f(a)$ for each $a \in A$;

② $f(a) \in B$ for each $a \in A$

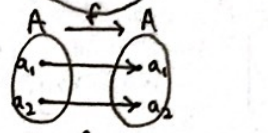
ARROW DIAGRAMS



COMMON FUNCTIONS

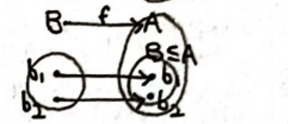
Identity function on A:

$\boxed{I_A: A \to A;\ a \mapsto a}$



Inclusion map of B in A:

$B \subseteq A.\ \boxed{\iota_B^A: B \to A;\ b \mapsto b}$



More Definitions

Floor of x: $\boxed{\lfloor x \rfloor := \max\{n \in \mathbb{Z} \mid n \leq x\}}$;

Ceiling of x: $\boxed{\lceil x \rceil := \min\{n \in \mathbb{Z} \mid x \leq n\}}$;

SEQUENCES

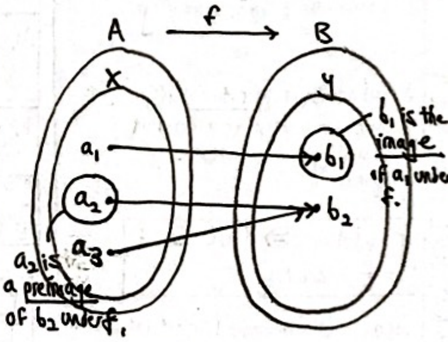
A sequence is a function whose domain is $\mathbb{Z}^+$.

We sometimes write a sequence as an infinite tuple:

$h: \mathbb{Z}^+ \to B$

$(h(1), h(2), h(3), \cdots) = (h(n))_{n \in \mathbb{Z}^+}$

IMAGES AND PREIMAGES



Let $X \subseteq A$ and $Y \subseteq B$. Then:

Set of images of X under f:

$f(X) := \{f(x) \mid x \in X\} = \{b \in B \mid \exists x \in X, f(x) = b\}$;

Set of preimages of Y under f:

$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$

Note that: $\boxed{a \in f^{-1}(Y) \Leftrightarrow f(a) \in Y.}$

RANGE

The range of f is the set of all images of f.

$\boxed{\mathcal{R}(f) := \{f(a) \mid a \in A\} = f(A)}$

- $\mathcal{R}(f) \subseteq B$ (codomain)
- $f(X) \subseteq \mathcal{R}(f)$ for all $X \subseteq A$.

To find $\mathcal{R}(f)$, make an intelligent guess on what it should be, (eg. set C), then prove that $C = \mathcal{R}(f)$.

(more info about functions on the next page)

EQUAL FUNCTIONS

Two functions f and g are equal, $\boxed{f=g}$, iff:

- Domains of f and g are equal
- Codomains of f and g are equal
- $f(x)=g(x)$ for all x in the domain of f (= domain of g)

COMPOSITE FUNCTIONS

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

Composition of f with g,

$$\boxed{\begin{aligned} g \circ f &: A \to C \\ a &\mapsto g(f(a)) \end{aligned}}$$

Codomain of f = Domain of g.

$\boxed{f^n \text{ denotes } \underbrace{f \circ f \circ \cdots \circ f}_{n}}$

$\boxed{f^0 \text{ denotes } I_A. \quad f^0(a)=a \text{ for all } a \in A}$

Associativity:

$\boxed{h \circ (g \circ f) = (h \circ g) \circ f}$

Not Commutative:

In general, $g \circ f \neq f \circ g$.

INVERSE FUNCTIONS

$f: A \to B$.

An inverse of f is a function $g: B \to A$ such that $\boxed{g \circ f = I_A}$ and $\boxed{f \circ g = I_B}$.

$\boxed{f \text{ has an inverse} \Leftrightarrow f \text{ is bijective}}$

The inverse of a bijective function is unique:

Suppose that $g, h: B \to A$ s.t. $g \circ f = I_A$ and $f \circ h = I_B$. Then $g=h$.

In other words: If g and h are both inverses of f, then $g=h$.

Inverse of f is denoted as $\boxed{f^{-1}}$.

CARDINALITY ☒

Cardinality of a set A, denoted $|A|$, is the size of A.

- A is finite → $|A|$ denotes no. of distinct elements in A.

For a function $f: A \to B$,

f is injective	$\to |A| \leq |B|$
f is surjective	$\to |A| \geq |B|$
f is bijective	$\to |A| = |B|$

☒ means non-examinable.

$|A| \leq |B| \Leftrightarrow$ There exists an injective function $f: A \to B$.

$|A| = |B| \Leftrightarrow$ There exists a bijective function $f: A \to B$

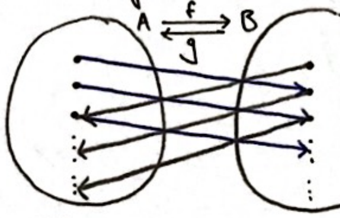
$\boxed{|A| < |\mathcal{P}(A)|}$

$\boxed{\text{Let } A \text{ be an infinite set. Then } |\mathbb{Z}^+| \leq |A|}$

CANTOR-BERNSTEIN THEOREM

Cantor-Bernstein Theorem:

Let $f: A \to B$ and $g: B \to A$ be injective functions. Then there exists a bijective function $h: A \to B$.



COUNTABILITY ☒

A set A is countable iff $\boxed{|A| \leq |\mathbb{Z}^+|}$.

A and B are countable sets $\Rightarrow A \times B$ is countable.

A finite product of countable sets, $A_1 \times A_2 \times \cdots \times A_n$, where $n \in \mathbb{Z}^+$, is also countable.

$\mathbb{Q}$ is countable.

A countable union of countable sets is countable.

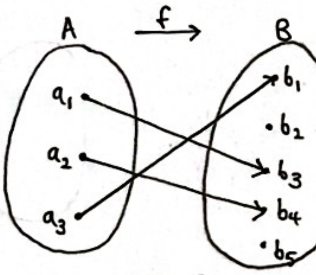
(I didn't summarise uncountable sets here 'cause no point)

• INJECTIVITY

A function $f: A \to B$ is injective (ie one-to-one) iff distinct elements of A have distinct images under f.

$\boxed{f \text{ is injective} \Leftrightarrow \forall a_1, a_2 \in A, (a_1 \neq a_2 \to f(a_1) \neq f(a_2))}$

$\boxed{f \text{ is injective} \Leftrightarrow \forall a_1, a_2 \in A, (f(a_1) = f(a_2) \to a_1 = a_2)}$ (*)



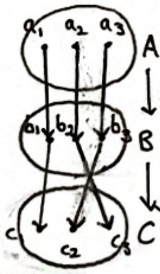
Additional Characteristic: No 2 arrows terminate at the same point in the codomain. (ie. one-to-one).

Proving that a function is injective:

Take two (general) elements $a_1, a_2 \in A$.

Assume that $f(a_1) = f(a_2)$.

Work towards the conclusion that $a_1 = a_2$.



Composition of Functions Preserves Injectivity:

$f: A \to B$ and $g: B \to C$.

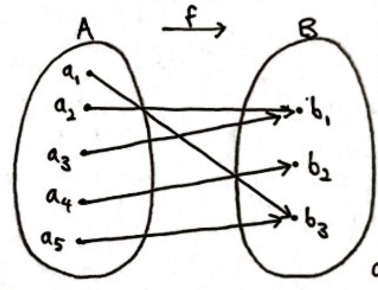
$\boxed{f \text{ and } g \text{ are both injective} \Rightarrow g \circ f \text{ is injective.}}$

$\boxed{g \circ f \text{ is injective} \Rightarrow f \text{ is injective.}}$

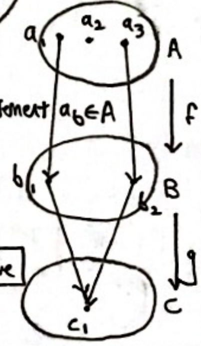
• SURJECTIVITY

A function $f: A \to B$ is surjective (ie. onto) iff its range equals its codomain, ie $\mathcal{R}(f) = B$.

$\boxed{f \text{ is surjective} \Leftrightarrow \forall b \in B, \exists a_b \in A, f(a_b) = b.}$



Additional characteristic: Every element in the codomain has at least one arrow terminating there.



Proving that a function is surjective:

Take a general element b of B, and find an element $a_b \in A$ such that $f(a_b) = b$.

Composition of functions preserves surjectivity:

$f: A \to B$ and $g: B \to C$.

$\boxed{f \text{ and } g \text{ are both surjective} \Rightarrow g \circ f \text{ is surjective}}$

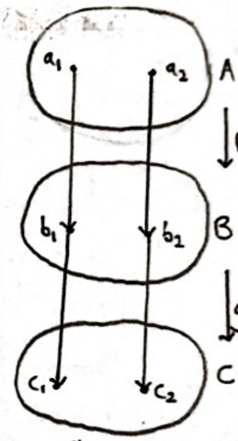
$\boxed{g \circ f \text{ is surjective} \Rightarrow g \text{ is surjective.}}$

Proving that a function is bijective: (Lemma) $f: A \to B$.

f is bijective $\Leftrightarrow$ for every $b \in B$, there exists a unique (**) $a_b \in A$ such that $f(a_b) = b$.

• BIJECTIVITY

A function is bijective iff it is both injective and surjective.



Composition of functions preserves bijectivity:

$\boxed{f \text{ and } g \text{ both bijective} \Rightarrow g \circ f \text{ is bijective}}$

$\boxed{g \circ f \text{ is bijective} \Rightarrow f \text{ is injective and } g \text{ is surjective}}$

MATHEMATICAL INDUCTION

Well-Ordering Principle of $\mathbb{Z}^+$: (or $\mathbb{Z}_{\geq k}$)

Every non-empty subset of $\mathbb{Z}^+$ has a minimal element.

Proof by Induction

To prove that $P(n)$ is true for all $n \in \mathbb{Z}^+$,

① Check that base case $P(1)$ is true.

Induction: ② Assume $P(n)$ is true.

Strong Induction: ② Assume that $P(1), P(2), \ldots, P(n)$ is true

③ Use this to prove that $P(n+1)$ is true.

Another form of MI: Let $k \in \mathbb{Z}^+$. For each $n \in \mathbb{Z}^+$, let $P(n)$ be a statement.

Suppose that $P(1), P(2), \ldots, P(k)$ are true, and that $(P(n) \wedge P(n+1) \wedge \cdots \wedge P(n+k-1) \to P(n+k))$ is true for all $n \in \mathbb{Z}^+$.

Then $P(n)$ is true for all $n \in \mathbb{Z}^+$.

} Useful for proving results about recursively defined sequences.

PRIME AND COMPOSITE NUMBERS

$n \in \mathbb{Z}^+$.

Prime numbers

n is prime $\Leftrightarrow$ $n \geq 2$ and n is not composite.

Composite numbers

n is composite $\Leftrightarrow \exists a, b \in \mathbb{Z}^+$ with $1 < a, b < n$ and $n = ab$

Existence of Prime Factorisation

Every $n \in \mathbb{Z}_{\geq 2}$ can be factorised into primes.

(ie. $n = p_1 p_2 \cdots p_k$ where $p_1, p_2, \ldots, p_k$ are primes, and $k \in \mathbb{Z}^+$).

Prepared by:
Joshua Chew Jian Xiong
@josuaaah

DISCRETE STRUCTURES. $\vee \wedge \sim \to \leftrightarrow$

CS1231S

1° RECURRENCE RN

Suppose that the sequence $a_1, a_2, \ldots$ of integers satisfies

$\boxed{a_{n+1} = ka_n + d}$ for all $n \in \mathbb{Z}^+$. $k, d \in \mathbb{R}$, $k \neq 0$.

Then converting to closed formula,

$$\boxed{a_n = \begin{cases} k^{n-1}a_1 + \dfrac{k^{n-1}-1}{k-1}d, & \text{if } k \neq 1; \\ a_1 + (n-1)d, & \text{if } k = 1 \end{cases} \quad \text{for all } n \in \mathbb{Z}^+.}$$

2° RECURRENCE RN.

Suppose that the sequence $a_1, a_2, \ldots$ of integers satisfies

$\boxed{a_{n+2} = sa_{n+1} + pa_n}$ for all $n \in \mathbb{Z}^+$. $s, p \in \mathbb{R}$, $p \neq 0$, $s^2 \geq -4p$.

Let α and β be the real roots of the quadratic equation $\boxed{x^2 - sx - p = 0.}$

$$\boxed{a_n = \begin{cases} A\alpha^n + B\beta^n, & \text{if } \alpha \neq \beta; \\ (Cn+D)\alpha^n, & \text{if } \alpha = \beta \end{cases} \quad \text{for all } n \in \mathbb{Z}^+,}$$

where $A, B, C, D \in \mathbb{R}$ satisfy:

$$\boxed{\begin{cases} A\alpha + B\beta = a_1 \\ A\alpha^2 + B\beta^2 = a_2 \end{cases} \quad \text{and} \quad \begin{cases} (C+D)\alpha = a_1 \\ (2C+D)\alpha^2 = a_2 \end{cases}}$$

RECURSIVELY-DEFINED SETS

A recursively-defined set consists of

· Base	$3 \in S$
· Recursion	for all $x, y \in S$, $x+y \in S$
· Restriction	No integer belongs to S other than those coming from the base and recursion

Recursively-defined sets are well-defined.

STRUCTURAL INDUCTION

For a recursively-defined set S, to prove that

$\boxed{\forall x \in S\ p(x)}$,

we use Structural Induction:

① Verify $p(b)$ for all $b \in B$, where B is the base of S.

② Show that $p(y)$ is true if y is obtained from $x_1, x_2, \ldots$ by applying a rule in the recursion of S and $p(x_1), p(x_2), \ldots$ are true.