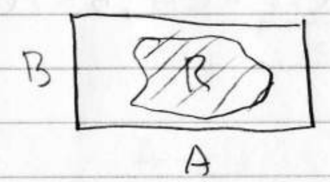
* Funcs and relations:

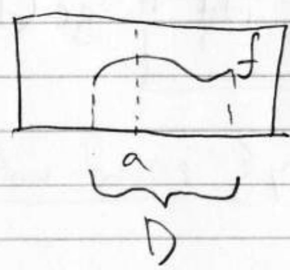
A, B sets $A \times B = \{(a,b) : a \in A, b \in B\}$
any $R \subseteq A \times B$ is a rel from $A \to B$.

$\to P(X) = 2^X = \{S : S \subseteq X\}$
↑ power set



- binary rel from A to B if $A = B$
- $\Rightarrow R$ is a binary rel on A

$\to$ Funcs: $f : A \to B$ is a function from A to B iff f is a rel. s.t. if $a \in A$ at most one $b \in B$ has $(a,b) \subseteq f$



- for any $a \in A$ at most one $b \in B$ has $(a,b) \in f$
- call it $f(a)$

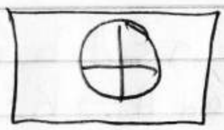
$$f = \{(a, f(a)) : a \in D\}$$

$\to$ Domain$(f) = \{a \in A : (a,b) \in f$ some $b\}$
$= \{a \in A :$ there is some $b = f(a)$ in $B\}$

$\to$ Domain$(R) = \{a :$ there is $b \in B$ $(a,b) \subseteq R\}$

ex: $A = B = \mathbb{R}$

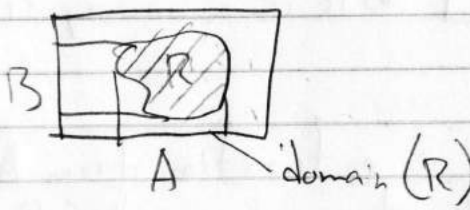
$R = \{(x,y) : x^2 + y^2 = 1\}$ ~~Domain~~ (R)



Domain $(R) = [-1, 1]$

$\rightarrow$ Range $(f) = \{b \in B :$ there is $a \in A, (a,b) \in f\}$

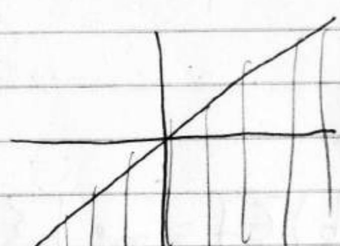
$= \{b \in B :$ there is $a \in A, b = f(a)\}$



*Def: $f : A \to B$ is <u>onto</u> iff range $(f) = B$ (surjective)

<u>ex.</u> $A = B = \mathbb{R}$

$R = \geq = \{(x,y) : x \geq y\}$



$\rightarrow (a,b) \in R \Rightarrow aRb$

<u>ex</u>: $P(X)$ X set

$A \subseteq B$

$\downarrow$

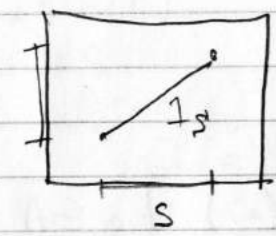
$\subseteq = \{(A,B) : A \subseteq B\} \Rightarrow \subseteq P(x) \circ P(X)$

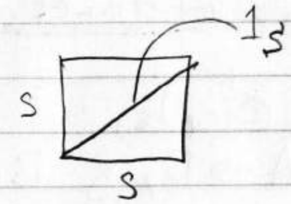
$A = B$

$\rightarrow$ '$=$' $= \{(A,B) : A \subseteq X, B \subseteq X, A = B\}$

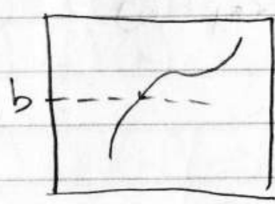
Let A be a set $S \subseteq A$

define 1_S on S by $1_S(s) = s$ all $s \in S$. $\mathrm{Dom}(1_S) = S$





*Def: $f : A \rightarrow B$ is 1-1 (injective) iff a_1, a_2 in A are equal if $f(a_1) = f(a_2)$



*Indicator funcs: $S \subseteq A$

$$I_S(a) = \begin{cases} 1 & \text{if } a \in S \\ 0 & \text{if } a \notin S \end{cases}$$

$I_S \in \{0,1\} = \{f : f : A \rightarrow \{0,1\}\}$, B^A

$\Downarrow$

domain$(f) = A$

*Def: $f : A \rightarrow B$ is a bijection or 1-1 correspondence iff f is 1-1 onto domain$(f) = A$

$S \to I_S$ is a bijection from $P(A)$ to $\{0,1\}^A = 2^A$

If $f \in \{0,1\}^A$ set, $S_f = \{a \in A : f(a) = 1\}$

$f = I_{S_f}$

Comp. of funcs:

A, B, C sets
$f: A \to B$, $g: B \to C$
funcs: $g \circ f(a) = g(f(a))\ \forall a \in A$ defines $g \circ f : A \to C$

(a,b) in graph (f) $(=f)$
(b,c) in graph (g) $(=g)$
implies that (a,c) in graph $(g \circ f)$

$c = (g \circ f)(a)$

R relation from A to B
S " " B to C

* $\underbrace{(a,c) \text{ is in } S \circ R}_{a(S \circ R)c}$ iff $\exists b \in B$ s.t. $\underbrace{(a,b) \in R}_{aRb}$, $\underbrace{(b,c) \in S}_{bSc}$

→ Let A, B, C be $\mathbb{Z}$, R, S be $>$.
If $a > b$, $b > c \Rightarrow a(> \circ >)c = a >> c$

$a > b$ $\quad$ $b > c$
means
$a \geq b+1$ $\quad$ $b \geq c+1$
$\therefore a \geq c+2 \Rightarrow a(> \circ >)c$

* **Thm:** Comp. of funcs. is associative.

→ Let $f: A \to B$, $g: B \to C$, $h: C \to D$ be funcs. Then
$h \circ (g \circ f) = (h \circ g) \circ f$

Pf: Let $d = h \circ (g \circ f)(a)$,
$\exists c \in C, d = h(c)$,
$(g \circ f)(a) = c$
$\exists b \in B$ w/ $c = g(b)$
$b = f(a)$

$d = h(c)$, $c = g(b)$
$\therefore d = (h \circ g)(b)$
also $f(a) = b$
$\therefore d = (h \circ g)(f(a))$
$= ((h \circ g) \circ f)(a)$

$(a,d) \in h \circ (g \circ f)$.
$\exists c: (c,d) \in h, (a,c) \in (g \circ f)$

$\exists b: (a,b) \in f, (b,c) \in g$

$(b,d) \in (h \circ g)$

$(a,d) \in (h \circ g) \circ f$
$(a,d) \in h \circ (g \circ f)$

If $d = ((h \circ g) \circ f)(a) \Rightarrow d = (h \circ (g \circ f)(a)$

* Identify funcs:

→ $f: A \to B \Rightarrow f \circ 1_A = f$, $1_B \circ f = f$

$(f \circ 1_A)(a) = f(1_A(a)) = f(a)$

→ if $A = B$: $1_A \circ f = f \circ 1_A = f$ any $f: A \to A$

* Thm: $f: A \to B$, $g: B \to C$
i) f, g are inj $\Rightarrow g \circ f$ is inj
ii) f, g are sur $\Rightarrow g \circ f$ is sur.
iii) f, g are bij $\Rightarrow g \circ f$ is bij.

iv) if $(g \circ f)$ is sur. $\Rightarrow g$ is sur.
v) if $(g \circ f)$ is inj. and range$(f) \subseteq$ domain(g)
$\Rightarrow f$ is inj.

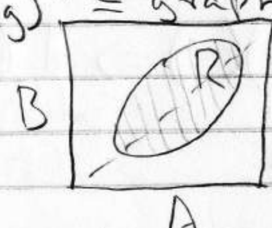
any $c \in C$ is $(g \circ f)(a)$ some a.
thus is $g(b)$ for $b = f(a)$

(*) Inv. funcs!

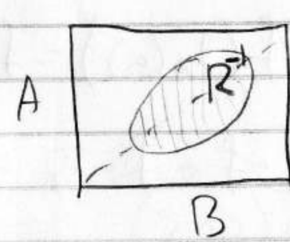
$$f : A \to B \Rightarrow \underbrace{g \circ f = 1_A}_{g \text{ left inv}} \text{ or } \underbrace{f \circ g = 1_B}_{g \text{ right inv}}$$

If $f(x) = y \Rightarrow x = g(y)$
$(x, y) \in \text{graph}(f) \Rightarrow (y, x) \in \text{graph}(g)$
$\text{graph}(f)^{-1} \subseteq \text{graph}(g)$
$\text{graph}(g)^{-1} \subseteq \text{graph}(f)$ ⊛

Let $R \subseteq A \times B$



has $R^{-1} \subseteq B \times A$
iff $R^{-1} = \{(b, a) : (a, b) \in R\}$



⊛ $\text{graph}(f)^{-1} = \text{graph}(g)$

$\boxed{407}$

* $g \circ f = 1_A$, 1_A is 1-1 so f is 1-1
$f \circ g = 1_B$, 1_B is onto so f in onto

$\therefore$ f is bij if f^{-1} exists

$\rightarrow$ graph(g) = graph$(f)^{-1}$

$\rightarrow$ graph$(f)^{-1}$ has vertical line property,
graph(f) has horizontal line property

* Thm: $f: A \to B$ has $f^{-1}: B \to A$ iff f is bij.

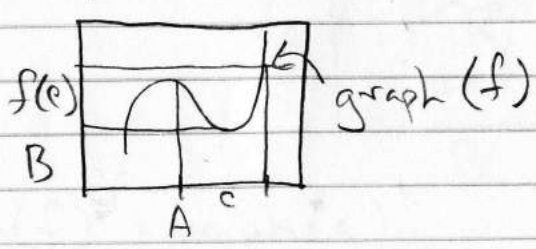
* Thm: f has inverse from range(f) to domain(f) iff f is 1-1

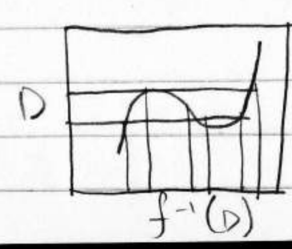
* Thm: Let $f: A \to B$ be bij. $h: B \to C$ as well $(h \circ f)^{-1} = f^{-1} \circ h^{-1}$

* Direct and inv. images under a func $f: A \to B$

def.: Let $C \subseteq A$, $D \subseteq B$. $f(C) = \{y \in B : y = f(x)$ some $x \in C\}$

$f^{-1}(D) = \{x \in A : f(x) \in D\}$





* Let $C_1 \subseteq C_2$ in A, $D_1 \subseteq D_2$ in B
Then $f(C_1) \subseteq f(C_2)$, $f^{-1}(D_1) \subseteq f^{-1}(D_2)$

$\rightarrow f^{-1}(D_1 \cup D_2) = f^{-1}(D_1) \cup f^{-1}(D_2)$

$\rightarrow f^{-1}(D_1 \cap D_2) = f^{-1}(D_1) \cap f^{-1}(D_2)$

$\rightarrow f(C_1 \cup C_2) = f(C_1) \cup f(C_2)$

$\rightarrow f(C_1 \cap C_2) = f(C_1) \cap f(C_2)$

- $C_1 \cup C_2 \supseteq C_1$, $C_1 \cup C_2 \supseteq C_2$ so
$f(C_1 \cup C_2) \supseteq f(C_1)$, $f(C_1 \cup C_2) \supseteq f(C_2)$

$\therefore f(C_1 \cup C_2) \supseteq f(C_1) \cup f(C_2)$

- Let $b \in f(C_1 \cup C_2)$. $\exists a \in C_1 \cup C_2$ w/ $f(a) = b$.
If $a \in C_1 \Rightarrow b \in f(C_1)$
If $a \in C_2 \Rightarrow b \in f(C_2)$

$\therefore b \in f(C_1) \cup f(C_2)$

* Let $A = B = \mathbb{R}$, $C_1 = (-\infty, 0]$, $C_2 = [0, \infty)$
Let $f(x) = x^2$, $f(C_1) = f(C_2) = [0, \infty)$
$\therefore f(C_1) \cap f(C_2) = [0, \infty)$
$C_1 \cap C_2 = \{0\}$
$f(C_1 \cap C_2) = f(\{0\}) = \{f(0)\} = \{0\}$

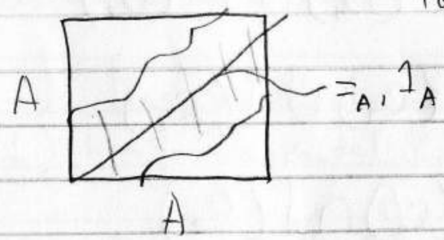
* Properties of rel. R on A:

i) Reflexivity: if $a \in A \Rightarrow aRa$, $(a,a) \in R$

$\therefore 1_A, =_A \subseteq R$

For any $a \in A$ aRa

For all a $(a,a) \in R$



$=_A$ smallest reflexive rel. $A \times A$ largest aRb, all a,b

ii) Symmetry: R is sym. if aRb implies bRa, $aR^{-1}b$

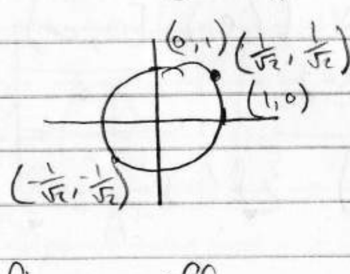
* Lemma: for any rel S, $(S^{-1})^{-1} = S$

$\rightarrow R \subseteq R^{-1}$, $R^{-1} \subseteq (R^{-1})^{-1}$

but $R^{-1} \subseteq R$

$\therefore R = R^{-1}$

Ex: in $\mathbb{R} \times \mathbb{R}$. $\{(x,y) : x^2 + y^2 = 1\}$



sym, but not ref.

* R is irreflexive iff no a has aRa $(>, \subset)$

* Asymmetric: aRb and bRa impossible

iii) Transitivity: R is transitive iff when aRb and bRc then aRc.

If $a(R \circ R)c$ then aRc. $\therefore R \circ R \subseteq R$

⊛ <u>Partial order:</u>

(Strong)
i) Transitive
+ ii) Irreflexive

Ex. $>$, $\subset$

Note if aRb and bRa then $a=b$ by trans.

* A total/complete/linear partial order is a partial order which satisfies for an $a \neq b$ either aRb or bRa

* <u>Trichotomy</u>: for $a,b \in A$ precisely one: aRb, $a=b$, or bRa.

---

* <u>ex.</u> A set $P(A)$ subsets $\{0,1\}^A$ funcs $f: A \to \{0,1\}$

$$S \in P(A) \Rightarrow I_S(a) = \begin{cases} 1 & a \in S \\ 0 & a \notin S \end{cases}$$

$I_S \in \{0,1\}^A$: define $S_f = \{a : f(a) = 1\} = \text{support}(f)$

$I: S \to I_S$
$S: f \to S_f$
$\Rightarrow S = I^{-1}$ (inverse)

- $A = \{1, 2, \dots, n\} \Rightarrow |\{0,1\}^A| = 2^n$

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

- A is inf. $\Rightarrow |P(A)| = 2^{|A|} = |\{0,1\}^A|$

- $A = \mathbb{N} \Rightarrow |P(\mathbb{N})| = |\{0,1\}^{\mathbb{N}}| = 2^{|\mathbb{N}|} = 2^{\aleph_0} > \aleph_0$

$$2^{|\mathbb{N}|} = c = |[0,1]|$$

☆ *Weak partial order:

i) Transitive

ii) Reflexive

(May impose: aRb and bRa implies $a=b$)

Ex. $\geq$, $\subseteq$

(*) Equivalence rel.:

i) Reflexive

ii) Symmetric

iii) Transitive

- Ex. $=_A$, $A \times A$

- Ex. Congruence of triangles in plane

$T_1 R T_2$, $T_2 R T_3$ then $T_1 R T_3$

$T_1 R T_2$ iff $\text{area}(T_1) = \text{area}(T_2)$

- Let $f: A \to B$ be a func. w/ domain$(A) = A$

  $a_1 \sim_f a_2$ iff $f(a_1) = f(a_2)$

Reflexive: $a \sim_f a$, $f(a) = f(a)$

Symmetric: $a \sim_f b$, $f(a) = f(b)$

$\therefore f(b) = f(a)$

$\therefore b \sim_f a$

Transitive: Let $a \sim_f b$ and $b \sim_f c$

then $f(a) = f(b)$ and $f(b) = f(c)$

$\therefore f(a) = f(c)$ or $a \sim_f c$

(*) Equivalence Classes:

R equivalence Relation on A $a \in A$

$$[a]_\sim = \{b \in A : a \sim b\}$$

$\parallel$

equivalence class of a modulo $\sim$

- Let $b \in [a]_\sim$. ($\therefore a \in [a]_\sim$)

  $\Rightarrow a \in [b]_\sim$ since $a \sim b$ implies $b \sim a$

Assert $[b]_\sim \subseteq [a]_\sim$

Let $c \in [b]_\sim$ so $b \sim c$. But $a \sim b$

$\therefore a \sim c$

$[a]_\sim \subseteq [b]_\sim$

$\therefore [a]_\sim = [b]_\sim$

Thm: Let $\sim$ be an equivalence rel. on A
$A/\sim = \{[a]_\sim : a \in A\}$ (factor set)
forms a partition of A.

i) $A = \bigcup \{[a]_\sim : a \in A\}$
ii) $[a]_\sim \cap [b]_\sim \neq \emptyset \Rightarrow [a]_\sim = [b]_\sim$

Pf: Let $c \in [a]_\sim \cap [b]_\sim$
then $[a]_\sim = [c]_\sim$
$[c]_\sim = [b]_\sim$

$\therefore$ Using trans of equality: $[a]_\sim = [b]_\sim$

---

* If $\sim$ is an equivalence relation on A
$\Rightarrow \{b : a \sim b\} = [a]_\sim$
$\{[a]_\sim : a \in A\}$ Partitions A

$f : A \to B$, domain$(f) = A \Rightarrow a_1 \sim_f a_2$ iff $f(a_1) = f(a_2)$

* $[a]_{\sim_f} = f^{-1}(b)$ if $b = f(a)$

$\{f^{-1}(b) : b \in B\}$ is factor set of all equivalence classes

* $P = \{A_i : i \in I\}$ be a partition of A.
Let $f(a) = c$ if $a \in A_i$, $f : A \to I$, $f^{-1}(i) = A_i$
if $f(a) = i$, $[a]_{\sim_f} = A_i$

⊛ A set theoretical model of $\mathbb{Z}^+$ or $\mathbb{N}$:

Def: A is a set $\Rightarrow S(A) = A+1 = A \cup \{A\}$

Def: $0 = \emptyset \Rightarrow S(0) = S(\emptyset)$

$\Rightarrow 1 = 0+1 = \{\emptyset\}$

$\Rightarrow 2 = 1+1 = S(1) = \{\emptyset\} \cup \{\{\emptyset\}\}$

$= \{\emptyset, \{\emptyset\}\} = \{0,1\}$

If $n = \{0,1,2,\dots,n-1\}$ then $n+1 = S(n) = \{0,1,2,\dots,n-1\} \cup \{\{0,1,2,\dots,n-1\}\}$

$= \{0,1,2,\dots,n-1\} \cup \{n\}$

$= \{0,1,2,\dots,n-1,n\}$

Def: A collection C of sets is inductive iff $A \in C$ implies $A+1 \in C$

$\mathbb{Z}^+$ is smallest inductive set containing 0.

$\mathbb{N} = \mathbb{Z}^+ \setminus \{0\}$ is smallest inductive set containing 1.

⊛ Principle of induction:

$A \subseteq \mathbb{Z}^+$ is $\mathbb{Z}^+$ iff i) $0 \in A$ and ii) if $n \in A \Rightarrow n+1 \in A$

i') $1 \in A$

Def: A sequence X is a function on $\mathbb{Z}^+$ (or $\mathbb{N}$) to some set $\underline{X}$

* Proof by induction: Let $(P_n)_{n=0}^{\infty}$ be a sequence of logical propositions. If

i) P_0 is true

ii) P_n is true $_{\text{all } k \leq n}$ implies P_{n+1} true then all P_n true

* Definition by induction: If i) x_1 is defined and given definition of x_n then x_{n+1} is defined, then $(x_n)_{n=1}^{\infty}$ is well defined.

* Let f be a func. from $A \to A$ (w/ domain A)

$$f^0 = I_A,\ f^1 = f,\ f^2 = f \circ f$$

$\forall n \in \mathbb{N}$ let $f^{n+1} = f^n \circ f$

<u>Thm:</u> $f_1 : A_1 \to A_2,\ f_2 : A_2 \to A_3, \dots, f_n : A_n \to A_{n+1}$

$$\Rightarrow \left((f_n \circ f_{n-1}) \circ \left((f_3 \circ f_2) \circ f_1 \right) \right.$$

$$\Rightarrow \left(f_n \circ \left(f_{n-1} \left(\dots \circ \left(f_3 \circ (f_2 \circ f_1) \right) \right) \right) \right.$$

$$\therefore f_3 \circ (f_2 \circ f_1) = (f_3 \circ f_2) \circ f_1$$

<u>Pf:</u> Suppose true for n funcs.
Look at $(n+1)$ funcs.

$$(f_{n+1} \circ \dots \circ f_{j+1}) \circ (f_j \circ \dots \circ f_1)$$

$$\Rightarrow \left(f_{n+1} \circ (f_n \circ \dots \circ f_{j+1}) \right) \circ \left(f_j \circ \dots \circ (f_2 \circ f_1) \right)$$

$$\Rightarrow f_{n+1} \circ \left(f_n \circ \left(f_{n-1} \circ \dots \circ f_{j+1} \right) \circ \left(f_j \circ \left(f_{j-1} \dots \left(f_2 \circ f_1 \right) \right) \right) \right)$$

$$\Rightarrow f_{n+1} \circ \left(f_n \circ \left(f_{n-1} \circ \dots \circ \left(f_j \circ \left(f_{j-1} \circ \dots \circ (f_2 \circ f_1) \right) \right) \right) \right)$$

* <u>Lemma:</u>

$$\begin{aligned} f^{n+1} &= f^n \circ f \\ &= (f^{n-1} \circ f) \circ f \\ &= (f \circ f^{n-1}) \circ f \\ &= f \circ (f^{n-1} \circ f) \\ &= f \circ f^n \end{aligned}$$

Thm: $f^{n+k} = f^n \circ f^k$
$= f^k \circ f^n$

Pf: $f^{k+1} \circ f^n$
$= (f \circ f^k) \circ f^n$
$= f \circ (f^k \circ f^n)$
$= f \circ (f^n \circ f^k)$
$= (f \circ f^n) \circ f^k$
$= (f^n \circ f) \circ f^k$
$= f^n \circ (f \circ f^k)$
$= f^n \circ f^{k+1}$

Def: $n = S^n(0)$

Def: $n+k = S^{n+k}(0)$ (addition of two integers)
(associative, commutative)

* $m \geq n$ iff $m = S^k(n)$, for some $k \in \mathbb{Z}^+$

* $m > n$
$l > m > n$ (transitivity)

* $(m+1) \cdot n = m \cdot n + n$ (recursive def. of multiplication)

Def: $m, n \in \mathbb{Z}^+$
$m \geq n$ iff $m = n + k$, for $k \in \mathbb{Z}^+$
$m > n$ iff $m = n + k$, for $k \in \mathbb{N}$

Thm: If $A (\neq \emptyset) \subseteq \mathbb{Z}^+$ then $\min(A)$ exists
Pf: Let L = lowerbds of A s.t. if $l \in L$, $a \in A$, $l \leq a$
$0 \in L$
Assume $\min(A)$ does not exist. Thus no $l \in L$ is in A.

407

If $a \in A$, $l < a$.
Thus $l+1 \leq a$ any $l \in L_1$
Thus $l+1 \in L_1$
$\therefore L_1 = \mathbb{Z}^+$ (contradiction)

Cor: Every lower bdd subset $A (\neq \emptyset)$ of $\mathbb{Z}$ has a min

Pf: If l lower bd $A - l = \{a - l ; a \in A\} \subseteq \mathbb{Z}^+$ has a min m
$m + l$ is lower bd of A.

Def: $\mathbb{N}_n = \{1, \dots, n\}$ initial segment of $\mathbb{N}$
$\{n, n+1, \dots\} = n + \mathbb{Z}^+$
Tail or final seg of $\mathbb{Z}^+$ or $\mathbb{N}$ if $n > 0$

Def. A set $A \neq \emptyset$ is finite iff $\exists n \in \mathbb{N}$ w/ $\mathbb{N}_n$ in 1-1 correspondence w/ A. In this case, we set $|A| = \text{card}(A) = \#A = n = \{0, 1, 2, \dots, n-1\}$

Thm: Let A be an infinite set. There is a non-repeating seq $(a_n)_{n=1}^{\infty}$ is A.

Pf: Let $A_1 = A$. Choose $a_1 \in A_1$. Set $A_2 = A_1 \setminus \{a_1\} \neq \emptyset$
else $A_1 = \{a_1\}$

Suppose distinct $a_1, a_2, \dots, a_n$ have been chosen from A.
$A_i = A \setminus \{a_1, \dots, a_{i-1}\}$ $\forall i \leq n$
$A_n = A \setminus \{a_1, \dots, a_{n-1}\} = A_n \setminus \{a_{n-1}\}$

$A_n \neq \emptyset$, else $A = \{a_1, \dots, a_{n-1}\} = \mathbb{N}_{n-1}$
Pick $a_n \in A_n$
Induction step

<u>Cor</u>: A_n infinite $\Rightarrow$ in 1-1 corresp. w/ a proper subset

Let $f : A \to A$
$f(a_i) = a_{i+1}$, $i \geq 1$
$f(a) = a$, $\forall a = a_i$, any i
$f(A) = A \setminus \{a\}$

<u>Thm</u>: There is no 1-1 corresp. btwn $\mathbb{N}_n$ and a proper subset.
<u>Pf</u>: $n = 1$ $\{1\} \Rightarrow \emptyset$ (trivial base case)
Assume true $n = k$.
Let $f : \mathbb{N}_{k+1} \to A \subseteq \mathbb{N}_{k+1}$ be 1-1 corresp.
i) $f(k+1) = k+1$
some $j \leq k$ in $\mathbb{N}_{k+1} \setminus A$
Let $g(i) = f(i)$ if $1 \leq i \leq k$
Then $g : \mathbb{N}_k \to (\mathbb{N}_k \setminus \{j\})$ (contradiction)
$\therefore$ case i) is imp.

ii) $f(k+1) \leq k$
Let $i = k+1$
Let $g(i) = k+1$
$g(k+1) = i$
$g(m) = m$, all others
$g : \mathbb{N}_{k+1} \to \mathbb{N}_{k+1}$

Look at $g \circ f : \mathbb{N}_k \to \mathbb{N}_k$

1-1 corresp. btwn $\mathbb{N}_k$ and $\text{range}(g \circ f) = g(A)$

$j \notin A$

$g(j) \notin g \circ f(\mathbb{N}_k)$

$\therefore$ $g \circ f$ 1-1 corresp. from $\mathbb{N}_{k+1}$ to $g(A) \neq \mathbb{N}_{k+1}$

$g \circ f(k+1) = k+1$ (back to case i contradiction)

① Cor: If $m < n$ there is no bij. $f : \mathbb{N}_n \to \mathbb{N}_m$

② Cor: $|A|$ is well defined unique n w/ A, $\mathbb{N}$ in 1-1 corresp.

$$\begin{tikzcd} \mathbb{N}_m \arrow[r, leftarrow, "g"] \arrow[r, bend right, "g^{-1}"'] & A \arrow[r, "f"] & \mathbb{N}_n \end{tikzcd}$$

$$\mathbb{N}_m \xrightarrow{f \circ g^{-1}} \mathbb{N}_n$$

Thm: There is no surjection from $\mathbb{N}_n$ to $\mathbb{N}_m$ if $m < n$

If $|A| = |B| = n$ in $\mathbb{N}$ and $f : A \to B$

i) f is bij

ii) f is inj

iii) f is sur

$\boxed{407}$

m, n integers

$m | n$ (m divides n, m is a divisor of n (factor)
n is a multiple of m)
iff $\exists k \in \mathbb{Z}$ s.t. $m \cdot k = n$

Rephrased: $n \in m\mathbb{Z} = \{mk : k \in \mathbb{Z}\}$
$m | n$ iff $(-m) | n$ iff $m | (-n)$

<u>Case 0:</u> $0 \cdot \mathbb{Z} = \{0k : k \in \mathbb{Z}\} = \{0\}$

$0 \cdot k$ if $k \neq 0$
$k \cdot 0 = 0$ so $k | 0$ $\forall k$

<u>Case 1:</u> $1 \cdot \mathbb{Z} = \{1 \cdot k : k \in \mathbb{Z}\}$
$= \mathbb{Z}$
$1 | k$ all k. But $k | 1$ iff $k = \pm 1$

* Note: divisibility is weak partial order (antisymmetric)
i) $n | n$ all n
ii) $n | m$ and $m | n$ implies $n = m$

If $m | n$ then $mk = n$ some k $|m||k| = |n|$
If $m, n \in \mathbb{Z}^+$, so is k
$m \cdot k = n$
$m \leq n$
iii) $l | m$, $m | n$ implies $l | n$
$m = lk'$, $n = mk$
$n = l(k'k)$
* Note: Suppose $m | n_1$, $m | n_2$ and that $\{a_1, a_2\}$ in $\mathbb{Z}$ then $m | (a_1 n_1 + a_2 n_2)$
↑ linear / integral combination

$m\mathbb{Z}$ "subspace" of $\mathbb{Z}$

$n_1 = mk_1$, $n_2 = mk_2$
$(a_1 n_1 + a_2 n_2) = a_1(k_1 m) + a_2(k_2 m) = (a_1 k_1 + a_2 k_2) m$

<u>Th 1.1.3 (Division Algorithm)</u>:

Let $a \in \mathbb{Z}$, $b \in \mathbb{N}$. There are unique ints q (quotient), r (remainder) w/ $a = bq + r$, $0 \leq r < b$

<u>Pf.: (Uniqueness)</u> $a = bq' + r'$, suppose $r' \leq r$

$bq + r = bq' + r'$
Thus, $r - r' = b(q - q')$
$0 \leq r - r' < b - 0 = b$
$r - r' = |r - r'| = |b||q' - q| = b|q' - q| \geq b$, if $|q' - q| \neq 0$
(contradiction)
$\therefore q' - q = 0 \Rightarrow q' = q \Rightarrow r = r'$

Let $R = \{r = a - bq : r \geq 0, q \in \mathbb{Z}\}$
$a - b(-|a|) \geq 0$
$a + b|a| \geq 0$
$a \geq -|a| \geq -b|a|$

$\therefore (r = a - b\underbrace{(-|a|)}_{(\geq 0)} \geq 0) \in R (\neq \emptyset) \subseteq \mathbb{Z}^+$

Let $r = \min(R)$, $a = bq + r$

$r < b$?
If not $r \geq b$, $r = r' + b$
$a = bq + (r' + b)$
$= b(q + 1) + r'$

But $r' < r = r' + b$, $r' \geq 0 \in R$ (contradiction)

$\therefore 0 \leq r < b$ ∎