Foundations Version 2.0

3.2 Equivalence Relations

Def: Let R be a relation on a set A. * R is <u>reflexive</u> if $aRa \ \forall a \in A$.

* R is <u>symmetric</u> if wherever aRb, then bRa
* R is <u>transitive</u> if wherever aRb and bRc, then aRc.

Ex $\leq$ on $\mathbb{R}$ * Is $\leq$ reflexive? Yes; $a \leq a \ \forall a \in \mathbb{R}$

* Is $\leq$ symmetric? No; $1 \leq 3$ but $3 \nleq 1$.
* Is $\leq$ transitive? Yes; If $a \leq b$ and $b \leq c$, then $a \leq c$.

Ex $\subseteq$ on $P(S)$ = set of all subsets of S

* reflexive? Yes; $A \subseteq A \ \forall A \in P(S)$
* symmetric? No: $S = \{1,2,3\}$, $A = \{1\}$, $B = \{1,2\} \Rightarrow A \subseteq B$ but $B \nsubseteq A$
* transitive? Yes: If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Ex $=$ on $\mathbb{Z}$

Clearly reflexive, symmetric, and transitive.

Ex: $A = \{1, 2, 3\}$

$R = \{(1,1), (2,2), (3,3), (1,2), (2,3)\}$

* Reflexive? Yes
* Symmetric? No: $(1,2) \in R$, but $(2,1) \notin R$
* Transitive? No: $1 R 2$ and $2 R 3$, but $1 \not R 3$

Def: A relation R on a set A is an equivalence relation if it is symmetric, reflexive, and transitive.

<u>Notation</u>: We will use $\sim$ to denote a general equivalence relation.

If $a \sim b$, we'll say a is equivalent to b.

Ex Let $A = \{$triangles in the Euclidian Plane$\}$

Consider geometric congruent, $\cong$.

* symmetric? Yes: if $\Delta_1 \cong \Delta_2$, $\Delta_2 \cong \Delta_1$
* reflexive? Yes; given any $\Delta \in A$, $\Delta \cong \Delta$
* transitive: yes: if $\Delta_1 \cong \Delta_2$ & $\Delta_2 \cong \Delta_3$, $\rightarrow \Delta_1 \cong \Delta_3$

Ex| Define ~ on $\mathbb{Z}$ by $a \sim b \leftrightarrow 6 \mid (b-a)$ Prove that ~ is an equivalent Rel.

Reflexivity: Let $a \in \mathbb{Z}$. since $0 = 0 \cdot 6$, we know that $6 \mid 0$. But $a-a=0$, so $6 \mid (a-a)$. Thus $a \sim a$.

Symmetric: Suppose $a \sim b$. Then $6 \mid (b-a)$, so $\exists k \in \mathbb{Z}$ s.t. $b-a = 6k$. Then $a-b = 6(-k)$. This implies $6 \mid (a-b)$, so $b \sim a$.

transitivity: Suppose $a \sim b$ and $b \sim c$. Then this means $6 \mid b-a$ and $6 \mid c-b$. Thus $\exists k, l \in \mathbb{Z}$ s.t. $b-a = 6k$ and $c-b = 6l$. Now $c-a = (c-b)+(b-a) =$
$= 6k + 6l = 6(k+l)$, so $6 \mid (c-a)$ and thus $a \sim c$.

Def: Let ~ be an equivalence relation on a set A and let $x \in A$.
The equivalence class of x, denoted $\bar{x}$ is the set $\bar{x} = \{y \in A \mid x \sim y\}$

Ex| Recall ~ defined on $\mathbb{Z}$ by $a \sim b$ iff $b \mid (b-a)$.

$0 \sim 0$ $\bar{0} = \{\ldots -12, -6, 0, 6, 12, \ldots\}$

$1 \sim 1$ $\bar{1} = \{\ldots -11, -5, 1, 7, 13, 18, \ldots\}$

similary,
$\bar{2} = \{\ldots -10, -4, 2, 8, 14, \ldots\}$

Similarly,
$\bar{2} = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$
$\bar{3} = \{\ldots, -9, -3, 3, 9, 15, \ldots\}$
$\bar{4} = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$
$\bar{5} = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$
$\bar{6} = \bar{0}$
$\bar{7} = \bar{1}$
So $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$, and $\bar{5}$ are all of the equiv. classes of ~.

Note: Every element a is in $\bar{a}$. Either $\bar{a} = \bar{b}$ or $\bar{a} \cap \bar{b} = \emptyset$. $\bigcup_{a \in \mathbb{Z}} \bar{a} = \mathbb{Z}$

Theorem: Let ~ be an equivalence relation on A, and let $x, y \in A$.
Then $x \in \bar{x}$. $\bigcup_{x \in A} \bar{x} = A$
$\bar{x} = \bar{y}$ or $\bar{x} \cap \bar{y} = \emptyset$.

Def: Let A be a set and let $\{B_\alpha\}_{\alpha \in I}$ be a family of subsets of A satisfying
1. $B_\alpha \neq \emptyset$ $\forall \alpha \in I$ 2. $B_\alpha \cap B_\beta = \emptyset$ or $B_\alpha = B_\beta$ 3. $\bigcup_{\alpha \in I} B_\alpha = A$
Then $\{B_\alpha\}_{\alpha \in I}$ is called a partition of A.

Ex| Using ~ as defined on $\mathbb{Z}$ previously, $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ is a partition of $\mathbb{Z}$.

Theorem: Equivalent class theorem: 1. Let ~ be an equivalent rel. on a set $A \neq \emptyset$. Then $C = \{\bar{x}\}_{x \in A}$ forms a partition of A. 2. Define ~ on A by $a \sim b$ iff $a, b \in B_\alpha$ for some $\alpha \in I$. Then ~ is an equivalent relation.

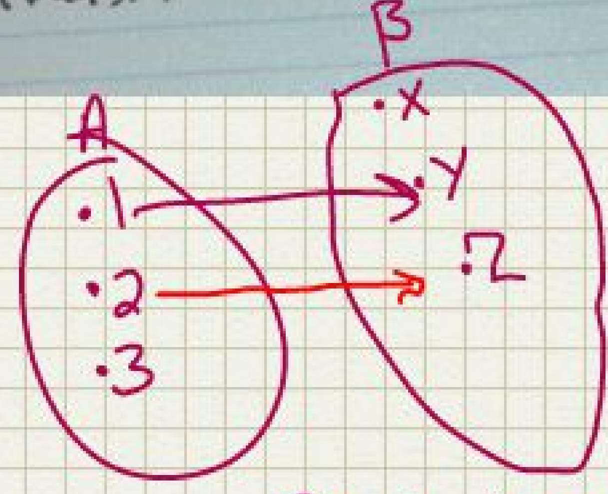
Tuesday, October 29, 2013
3:14 PM

Fact: Let R_1 and R_2 are equiv. relations on A.
1. $R_1 \cap R_2$ is an equiv. rel.
2. $R_1 \cup R_2$ is reflexive and symmetric (but not necessarily transitive).

For R from A to B w/ $S \subseteq Dom(R)$

$T \subseteq Ran(R)$

Prove $S \subseteq R^{-1}(R(S))$



R from A to B

$S \subseteq A \quad T \subseteq B$

$S = \{1\ 2\ 3\}$

$R = \{(1,3),(1,4)(2,4)(3,3)(17,0)\}$

$R(S) = \{3,4\}$

$R^{-1}(\{3,4\}) = \{1,2,3\}$

$S = \emptyset \quad R(\emptyset) = \emptyset$

$R^{-1}(\emptyset) = \emptyset$

$S = \{18\} \quad R(S) = \emptyset$

$R^{-1}(\emptyset) = \emptyset$

$\emptyset \neq S$ ▫

$S = 2,3$

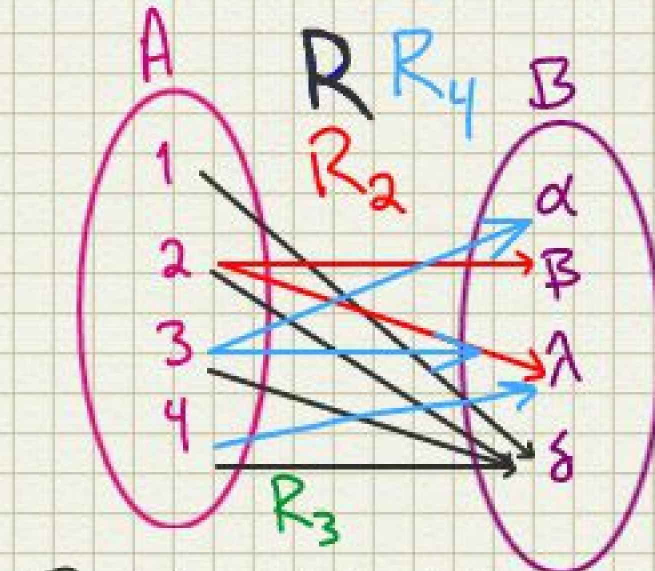
$R = (1,y)(2,Z)$

$R = (1,y)$

$R(S) = y, z$

$Dom\ R = \{1,2\}$

$Ran(R) = \{y, z\}$



$R_3 = \{\}$
$\text{Dom} R_3 = \emptyset = S$
$\text{Ran} R_3 = \emptyset = T$
$R^{-1}(R_3(S)) = R^{-1}(\emptyset) = \emptyset = S$

$R_4 = \{(3,\alpha), (3,\lambda)(4,\lambda)\}$
$\text{Dom } R_4 = \{3,4\} = S$
$\text{Ran } R_4 = \{\alpha, \lambda\} = T$
$R_4^{-1}(R_4(S)) = R_4^{-1}(\{\alpha,\lambda\}) = \{3,4\} = S$

3a) Now $(x,y) \in R$ where $x \in S$
$y \in R(S) \to x \in R^{-1}(R(S))$

$ARB = \{(1,\delta),(2,\delta),(3,\delta),(4,\delta)\}$
$\text{Dom} R = \{1,2,3,4\} = S$
$\text{Ran } R = \{\delta\} = T$
$R^{-1}(R(S)) = R^{-1}(\delta) = \{1,2,3,4\} = S$

$AR_2B = \{(2,B),(2,\lambda)\}$
$\text{Dom} R_2 = \{2\} = S; \text{Ran} R_2 = \{B,\lambda\} = T$
$R_2^{-1}(R_2(S)) = R^{-1}(B,\lambda) = \{2\} = S$

$(a,b) \wedge (b,c) \to (a,c)$
$(1,2) \wedge (2,2) \to (1,2)$
$(1,1) \wedge (1,2) \to (1,2)$

#11)
Let $a \in A$. Since $\text{Dom}(R) = A$, then $a \in \text{Dom}(R)$. $(a,b) \in R$ for some $b \in B$.
Then $(b,a) \in R$. By symmetry, $(a,a) \in R$. For $\text{Dom}(R) = A$, (a,a)

$(a,b) R (c,d) \leftrightarrow (a-c) \in \mathbb{Z}$ and $(b-d) \in \mathbb{Z}$

$(c,d) R (c-d) \to$ $c-c=0$, $d-d=0$ ✓

HW5 #3. Let $R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid |a-b| < 5\}$
$R = \{\ldots(-99,-98), \cdots (-4,0), (0,4), (98,99)(99,98)\ldots\}$
symmetric
$R = \{\ldots, (3,3), (99,99), (0,0), \ldots\}$ $(a,a) \in R \ \forall a \in \mathbb{Z}$
reflexive
$a-a=0$
$R = \{(8,4),(4,0)\}$ $|8-0| \nless 5$ NOT transitive
$R = \{(3,7),(7,3)\} \wedge 7 \neq 3 \therefore$ NOT Antisymmetric

$(a,b) R (c-d) \leftrightarrow (c,d) R (a,b)$

$a-c \in \mathbb{Z} \leftrightarrow c-a \in \mathbb{Z}$ ✓

3.3 Properties of relations on a set:

Def: Let R be a relation on a set A.

- R is <u>irreflexive</u> if $a \not R a\ \forall a \in A$
- R is <u>asymmetric</u> if aRb implies $b \not R a$.
- R is <u>antisymmetric</u> if aRb and bRa implies $a=b$.

Ex $\subseteq$ on $P(S)$

- irreflexive? No: If $A \subseteq S$, then $A \subseteq A$
- asymmetric? No: $A \subseteq A$ does not imply $A \not\subseteq A$
- antisymmetric? Yes. If $B \subseteq A \wedge A \subseteq B$, $A=B$

Ex $\leq$ on $\mathbb{Z}$

Irreflexive? No: $1 \leq 1$

Asymmetric? No: $1 \leq 1$ does not imply $1 \not\leq 1$.

antisymmetric? Yes: $a \leq b \wedge b \leq a$, $a=b$

Ex $<$ on $\mathbb{Z}$

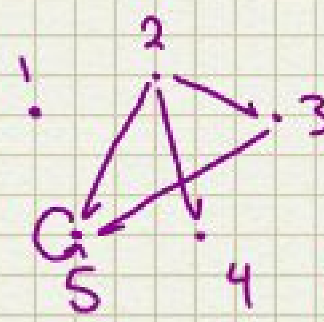
irreflexive? Yes: $a \not< a\ \forall a \in \mathbb{Z}$

asymmetric? yes: if $a<b$, then $b \not< a$

4b) Let $A=\{1,2,3,4,5\}$ and $R=\{(2,3),(2,4),(3,5),(2,5),(5,5)\}$

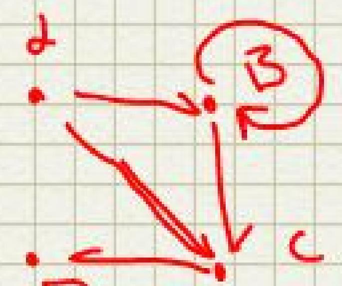
Ex $\subset$ on $P(S)$

- irreflexive? Yes: If $A \subseteq S$, then $A \not\subset A$
- asymmetric? yes: If $A \subset B$, then $B \not\subset A$
- antisymmetric? yes.



(D,D)

(C,B), (D,C), (C,a)



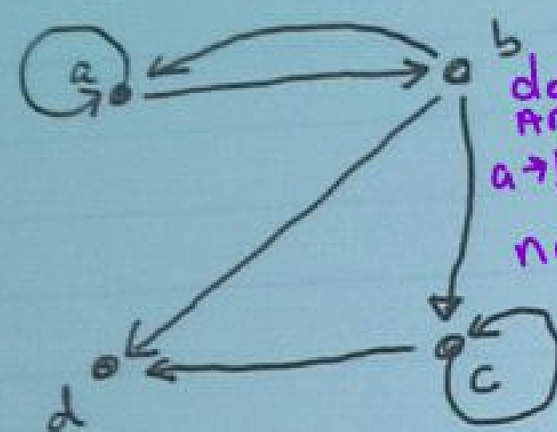
(a,B) (B,B), (B,C) (a,C), (C,d)

Digraphs of Relations

A digraph of a relation R on a set A is a way to visualize the properties of R.

- Nodes of the digraph corresponds to the elements of A.

Ex: Make a digraph of $R=\{(a,a),(c,c),(a,b),(b,a),(b,d),(c,d),(b,c)\}$ on $A=\{a,b,c,d\}$.



Reflexive? X

double arrows ↔ Symmetric? X

$a \to b$; $b \to c$ transitive? X No $a \to c$

no loops irreflexive? X

asymmetric? X

antisymmetric? X $a \neq c$

3.4: Orderings

<u>Def</u>: a relation R on a set A is a <u>partial order</u> of A if R is reflexive, antisymmmtric, and transitive.

<u>Notation</u>: $\prec$ will denote general partial order.

Examples: $\leq$ on $\mathbb{Z}$, $P(S), \subseteq$

$y R b R x$

$\forall b \in B,\ x, y \in A,\ B \subseteq A, R$ is a Poset.

Define R on $\mathbb{Z} - \{0\}$ by aRb if $a|b$

reflexive? yes; $a|a\ \forall a \in \mathbb{Z}$

antisymmetry? Does $a|b$ and $b|a$ imply $a=b$?
No: $2|-2$ and $-2|2$, but $2 \neq -2$.

Transitivity? Yes: If $a|b$ and $b|a$ then $a|C$, see test #1.

<u>Def</u>: Let $(A, \prec)$ be a poset. Then $\prec$ is a <u>linear order</u> of A if $\forall a, b \in A$, either $a \prec b$ or $b \prec a$.

<u>Ex</u>) $(\mathbb{Z}, \leq)$ is a linear order.

<u>Ex</u>) Define $\ll$ on $\mathbb{N}$ by $a \ll b$ iff $a|b$
is $\ll$ a linear ordering?
1. Is it a poset? Yes
2. But it is not linear order: $2 \not\ll 3$ and $3 \not\ll 2$

a) If R_1 and R_2 are irreflexive, Prove $R_1 \cap R_2$ and $R_1 \cup R_2$ are as well.

Let $a \in R_1$. Then $a \not R_1 a\ \forall a \in A$.
Let $b \in R_2$. Then $b \not R_2 b\ \forall b \in A$.
so $a \cancel{R_1 \cup R_2} a$
and $\exists a \in R_1 \cup R_2$ s.t. $a, a \notin R_1$ ~~bd~~ R_2

<u>Def</u>: Let $\prec$ be a partial order of $A \neq \emptyset$.

* $x \in A$ is maximal if $\nexists a \in A - \{x\}$ s.t. $x \prec a$.
* $x \in A$ is a maximum if $a \prec x\ \forall a \in A$
* $x \in A$ is minimal if $\nexists a \in A - \{x\}$ s.t. $a \prec x$
* $x \in A$ is a minimum if $\forall a \in A$, $y \prec a$.

$\ll$ "divides"

Ex] $A \neq \emptyset$. Consider $(P(A), \subseteq)$.

minimal: $\emptyset$ every subset of A contains $\emptyset$.

minimum elements: $\emptyset$

maximal elements: A

maximal element: A (A contains every subset of P(A)).

Fact: Let $\prec$ be a partial order of set $A \neq \emptyset$.

If $m \in A$ is a minimum, m is unique.

If $M \in A$ is a maximum, M is unique.

Proof | Suppose m_1, m_2 are minimum elements of A w.r.t. $\prec$.

m_1 is a minimum $\Rightarrow m_1 \prec m_2$
m_2 is a minimum $\Rightarrow m_2 \prec m_1$
} By antisymmetry, $m_1 = m_2$

Definition: Let $(A, <)$ be a linearly ordered set. If each non-empty subset of A contains a minimum element, then $(A, <)$ is a well ordered set.

Ex] $(\mathbb{N}, \leq)$ is well ordered set {well ordering Axiom.}

$(\mathbb{R}, \leq)$ is not well ordered.

$(-\infty, 0]$: no min

$(0, 1)$: no min

Onto functions

f is onto if $\forall b \in B\ \exists a \in A$ such that $f(a) = b$

Least Upper bounds // Greatest lower bound.

4.1: Functions - Basic Definitions

Def: x only paired with Y.

$f: A \to B$

Function f maps A to B.

$Dom(f) = A$; $Ran(f) \subseteq B$.

Prove F is a function:

Suppose $(x, y_1) \in F$ and $(x, y_2) \in F$

$(x, y_1) \in F \Rightarrow y_1 = 2x - 13$

$(x, y_2) \in F \Rightarrow y_2 = 2x - 13$ ■

Cardinality of Sets:

Two sets A and B have the same cardinality if $\exists$ bijection $f: A \to B$. A is countable if $\exists$ injection $f: A \to \mathbb{N}$

Fact: $\mathbb{Z}$ is countable. In fact, $|\mathbb{Z}| = |\mathbb{N}|$

Proof: Define $f: \mathbb{Z} \to \mathbb{N}$ by $f(z) = \begin{cases} -2z & \text{if } z < 0 \\ 2z+1 & z \geq 0 \end{cases}$

Fact: $\mathbb{R}$ is not countable

"Proof" Suppose $\mathbb{R}$ is countable. Then $\exists$ bijection $f: \mathbb{R} \to \mathbb{N}$. Then you can "number" the real #'s. In fact, you could number the reals in $(0,1)$.

Definition 4.15. A function $f: A \to B$ that is both one-to-one and onto is a ***one-to-one correspondence*** (or ***bijection***).

Definition 4.16. Let A be any nonempty set and define $I_A(x) = x$ for all $x \in A$. This function is a one-to-one correspondence and is called the ***identity function*** on A.

We will take the opportunity here to introduce some notation that will be studied in greater detail in Chapter 5. $\mathcal{F}(A)$ will represent the set of all functions from a nonempty set A to itself. $\mathcal{S}(A)$ will be used to represent the subset of $\mathcal{F}(A)$ whose elements are one-to-one and onto. $\mathcal{S}(A)$ is always nonempty since the identity function on A is an element of the set (since $A \neq \emptyset$).

Example 4.17. Let $A = \{a, b\}$. Define all functions on A as follows:

$\rightarrow$	I	f	g	h
a	a	a	b	b
b	b	a	b	a

Table 7: $\mathcal{F}(A)$ where $A = \{a, b\}$

We have $\mathcal{F}(A) = \{I, f, g, h\}$ and $\mathcal{S}(A) = \{I, h\}$ (Here, the table is read that $f = \{(a, a), (b, a)\}$, etc.)

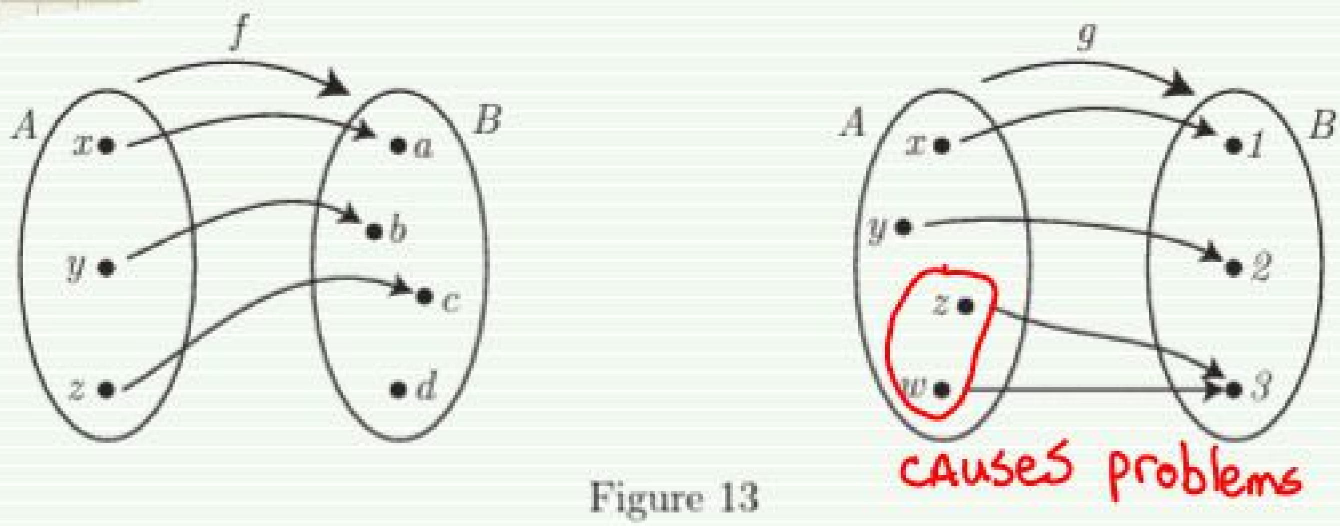


Figure 13

In Figure 13 we wee that $f : A \to B$ and the arrows of f can be reversed so that f^{-1} is a function from B to A; however, f^{-1} is not defined for all values of B and so we could not write $f^{-1} : B \to A$. If we restrict the domain, we could write $f^{-1} : \{a, b, c\} \to A$ or $f^{-1} : \mathrm{Ran}(f) \to A$.

With the function g indicated in 13 we encounter a more serious problem. Notice that z and w are both mapped to 3 by the function g. Therefore, reversing the direction of the arrows would map 3 to both z and w, a violation of the definition of a function. ***Thus it is clear that while all functions have inverses, the inverses may not be functions.*** We will consider the properties a function must have to possess an inverse function. We will call such a function ***invertible***.

Global Hypothesis

Theorem 4.18. *Let $f : A \to B$. Then $f^{-1} : Ran(f) \to A$ if and only if f is one-to-one.*

Proof. Suppose $f : A \to B$ and recall that this means f is a function, $\mathrm{Dom}(f) = A$, and $\mathrm{Ran}(f) \subseteq B$.

($\Leftarrow$): Assume f is one-to-one. To prove that $f^{-1} : \mathrm{Ran}(f) \to A$, we must establish that f^{-1} is a function, $\mathrm{Dom}(f^{-1}) = \mathrm{Ran}(f)$, and $\mathrm{Ran}(f^{-1}) \subseteq B$.

- First, to show that f^{-1} is a function, suppose (b, a_1) and (b, a_2) are elements of f^{-1}. Then (a_1, b) and (a_2, b) are elements of f. Since f is one-to-one, $a_1 = a_2$. Therefore f^{-1} is a function.
- Note that since f is a relation we have $\mathrm{Dom}(f^{-1}) = \mathrm{Ran}(f)$ (by Fact 3.10).
- Finally, since f is a relation, we have $\mathrm{Ran}(f^{-1}) = \mathrm{Dom}(f) = A$, so $\mathrm{Ran}(f^{-1}) \subseteq A$ (also by Fact 3.10).

(we used double containment) $\rightsquigarrow$ Tegrity

($\Rightarrow$): Assume $f^{-1} : \mathrm{Ran}(f) \to A$. Then f^{-1} is a function. To prove that f is one-to-one, suppose $(a_1, b), (a_2, b) \in f$. Then $(b, a_1), (b, a_2) \in f^{-1}$, and by virtue of f^{-1} being a function we can conclude that $a_1 = a_2$. Therefore, f is one-to-one. $\square$

f^{-1} is a function: Suppose $b_1, b_2 \in \mathrm{Dom}(f^{-1})$ with $b_1 = b_2$

$b_1 \in \mathrm{Dom}(f^{-1}) \to \exists\, a_1 \in \mathrm{Ran}(f^{-1}) \subseteq A$ s.t. $(b_1, a_1) \in f^{-1}$.

$b_2 \in \mathrm{Dom}(f^{-1}) \to \exists\, a_2 \in \mathrm{Ran}(f^{-1}) \subseteq A$ s.t. $(b_2, a_2) \in f^{-1}$.

$(a_1, b_1) \in f$ and $(a_2, b_2) \in f$. $b_1 = b_2$ and f is 1-1 $\to a_1 = a_2 \to f^{-1}(b_1) = f^{-1}(b_2)$ ∎

4.3 Combining functions, relations

Let R be a relation from A to B and let S be a relation from B to C.
The composition of R and S, $R\circ S$, is the relation from A to C defined by
$S\circ R=\{(a,c)\in A\times C \mid \exists\, b\in B \text{ with } (a,b)\in R \text{ and } (b,c)\in S\}$

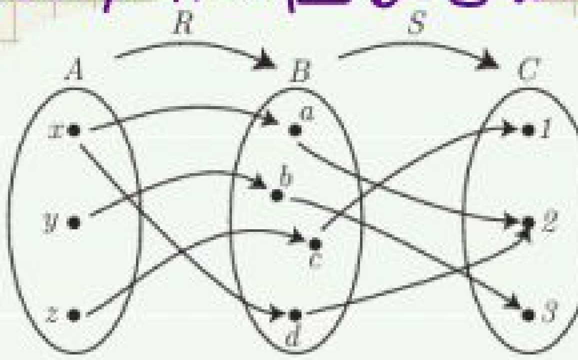


Figure 14: R is a relation from A to B and S is a relation from B to C.

Fact: Suppose $f: A\to B$ and $g: B\to C$.
Then $g\circ f: A\to C$

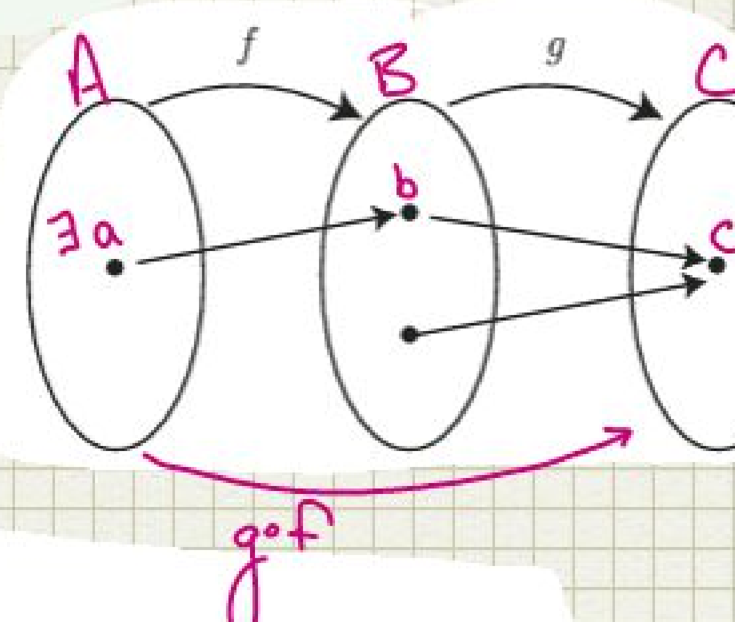
"Proof:" Let $f: A\to B$ and $g: B\to C$. To prove $g\circ f: A\to C$, we must show (1) $\mathrm{Dom}(g\circ f)=A$,
(2) $\mathrm{Ran}(g\circ f)\subseteq C$
(3) $g\circ f$ is a function.

Definition 4.20. Let R be a relation from A to B and S be a relation from B to C. Then the ***composition*** of R and S, denoted $S\circ R$, is defined by

$$S\circ R=\{(a,c)\in A\times D \mid \exists b\in B \text{ with } (a,b)\in R \text{ and } (b,c)\in S\}.$$

Theorem 4.27. *Let $f: A\to B$ and $g: B\to C$. Then*

1. *If f and g are one-to-one, then $g\circ f$ is one-to-one.*
2. *If f and g are onto, then $g\circ f$ is onto.*



Theorem 4.29. *Let $f: A\to B$ and $g: B\to C$.*

1. *If $g\circ f$ is one-to-one, then f is one-to-one.*
2. *If $g\circ f$ is onto, then g is onto.*

Proof.

1. Assume $g\circ f$ is one-to-one. To see f is one-to-one, let $f(a_1)=f(a_2)$. Then since g is a function, we have $g(f(a_1))=g(f(a_2))$. This implies $(g\circ f)(a_1)=(g\circ f)(a_2)$. Since $g\circ f$ is one-to-one, we have $a_1=a_2$. Therefore, f is one-to-one.
2. Assume $g\circ f$ is onto. To see g is onto, let $c\in C$. Since $g\circ f$is onto, there exists some $a\in A$ such that $(g\circ f)(a)=c$, and $(g\circ f)(a)=g(f(a))$. But $f(a)=b$ for some $b\in B$ and for that b we have $g(b)=c$. Therefore, g is onto

Recall $\mathcal{S}(A)=\{f: A\to A \mid f \text{ is bijective}\}$
some nice facts about $\mathcal{S}$

1. $\circ$ is a binary operation
2. $\circ$ is associative
3. $\circ$ has a special identity

7. Let $f : \mathbb{R} \to \mathbb{R}$. We say f is strictly increasing if $a < b$ implies $f(a) < f(b)$. Prove that if f is strictly increasing, then f is one-to-one and f^{-1} is strictly increasing.

Suppose f is increasing. Let $x_1, x_2 \in \mathrm{Dom}(f) = \mathbb{R}$ s.t. $f(x_1) = f(x_2)$.
Suppose $x_1 \neq x_2$, and WLOG suppose $x_1 < x_2$. f increasing implies $f(x_1) < f(x_2)$ #

If $y_1 < y_2$ then $f^{-1}(y_1) < f^{-1}(y_2)$

$(y_1, x_1), (y_2, x_2) \in f^{-1} \to (x_1, y_1), (x_2, y_2) \in f$.

We have $y_1 < y_2$ and f is inc.
if $x_1 \geq x_2 \xrightarrow[f\,\mathrm{inc}]{} y_2 \geq y_1$ #
so $x_1 < x_2$.

13 $f : A \to B$ $g : B \to C$ $g \circ f$ is onto and g is 1-1 $\longrightarrow$ f is onto

Proof: Let $b \in B = \mathrm{Dom}\, g \Rightarrow \exists c \in C$ s.t. $(b, c) \in g$.
$c \in C$ and $g \circ f$ onto $\Rightarrow \exists a \in A$ s.t. $(a, c) \in g \circ f$.
$(a, c) \in g \circ f \Rightarrow \exists \hat{b} \in B$ s.t. $(a, \hat{b}) \in f$ and $(\hat{b}, c) \in g$.
$(b, c), (\hat{b}, c) \in g$ and g 1-1 $\Rightarrow \underline{\underline{b = \hat{b}}}$. So $(a, \hat{b}) = (a, b) \in f$
Thus f is onto.

Fact 4.30. Let $f : A \to B$ and $g : B \to C$. If $g \circ f$ is 1-1 and f is onto, then g must be 1-1.

Fact 4.31. Let $f : A \to B$ and $g : B \to C$. If $g \circ f$ is onto and g is 1-1, then f must be onto.

4.4 More Properties of functions/relation

Fact 4.35: Let R be a relation from A to B and S a relation from B to C. Then $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Proof: {double containment}

($\subseteq$) Let $(c,a) \in (S \circ R)^{-1}$. Then $(a,c) \in S \circ R$.
By def. of $\circ$, $\exists b \in B$ s.t. $(a,b) \in R$ and $(b,c) \in S$.
Thus, $(b,a) \in R^{-1}$ and $(c,b) \in S^{-1}$. Since $(c,b) \in S^{-1}$ and $(b,a) \in R^{-1}$, then by def. of $\circ$, $(c,a) \in R^{-1} \circ S^{-1}$.

($\supseteq$) Let $(c,a) \in R^{-1} \circ S^{-1}$

Fact 4.36: Let R be a relation on R. ① R is symmetric iff $R = R^{-1}$
② R is transitive iff $R \circ R \subseteq R$.

Proof: ②

$\Rightarrow$ Suppose R is transitive and let $(a_1, a_3) \in R \circ R$. So $\exists a_2 \in A$ s.t. $(a_1, a_2) \in R$ and $(a_2, a_3) \in R$. By transitivity, $(a_1, a_3) \in R$.
Therefore, $R \circ R \subseteq R$

$\Leftarrow$ suppose $R \circ R \subseteq R$. Further suppose (a,b) and $(b,c) \in R$. By def. of $\circ$, $(a,c) \in R \circ R \subseteq R$. So $(a,c) \in R$. R is transitive.

P	Q	① $(P \rightarrow Q)$	② $(Q \rightarrow P)$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

①∧②	$P \leftrightarrow Q$	①∧② $\leftrightarrow (P \leftrightarrow Q)$
T	T	T
F	F	T
F	F	T
T	T	T

P	Q	R
T	T	
T	T	
T	F	
T	F	
F	T	
F	T	
F	F	T
F	F	F

Let $f: A \to B$, $T_1, T_2 \subseteq B$

$\to f^{-1}(T_1 \cap T_2) = f^{-1}(T_1) \cap f^{-1}(T_2)$.

Proof: Let $a \in f^{-1}(T_1 \cap T_2)$. Then $\exists t \in T_1 \cap T_2$ s.t. $(a,t) \in f$.

($\subseteq$) $t \in T_1 \cap T_2 \to t \in T_1$ and $t \in T_2$. $(a,t) \in f$ and $t \in T_1 \to a \in f^{-1}(T_1)$, and $a \in f^{-1}(T_2)$
$t \in T_2$

$\to a \in f^{-1}(T_1) \cap f^{-1}(T_2)$.

($\supseteq$) suppose $a \in f^{-1}(T_1) \cap f^{-1}(T_2)$.

$\to$ $a \in f^{-1}(T_1)$ and $a \in f^{-1}(T_2)$.

$a \in f^{-1}(T_1) \to \exists t_1 \in T_1$ s.t. $(a,t_1) \in f$

$a \in f^{-1}(T_2) \to \exists t_2 \in T_2$ s.t. $(a,t_2) \in f$

f is a function so $t_1 = t_2$

$(a,t_1), (a,t_2) \in f$ and f is a function $\to t_1 = t_2$. Let $t = t_1 = t_2$.

Now $(a,t) \in f$ and $t \in T_1 \cap T_2$. Since $t = t_1 \in T_1$, $t = t_2 \in T_2$. $a \in f^{-1}(T_1 \cap T_2)$

4.37(10): $(f \circ f^{-1})(T_1) \subseteq T_1$ with $f: A \to B$, $T_1 \subseteq B$.

Proof: Let $b \in (f \circ f^{-1})(T_1)$. Then $\exists t \in T_1$ s.t. $(t,b) \in f \circ f^{-1}$. By def. of $\circ$, $\exists a \in A$ s.t. $(t,a) \in f^{-1}$ and $(a,b) \in f$. Then $(a,t) \in f$. So $t = b$. since $t \in T_1$, so is b. ∎

Fact 4.39 stuff.

Chapter 5 - Binary Operations.

5.1 Basic Definitions

Def 5.1: Let S be a non-empty set. If $*: S \times S \to S$, then $*$ is called a Binary Operation on S.

Ex) "+" is a binary op. on $\mathbb{Z}$

Notation: If $(s_1, s_2) \in S \times S$, $*((s_1, s_2)) = s_1 * s_2$

Define $*$ on $\mathbb{Q}$ by $\frac{a}{b} * \frac{c}{d} = \frac{a+c}{b}$. Is it a binary operation on $\mathbb{Q}$?

No: $*$ is not a function: $\frac{1}{2} * \frac{1}{1} = \frac{1+1}{2} = 1$ but $\frac{2}{4} * \frac{3}{3} = \frac{3+2}{4} = \frac{5}{4}$ #

Fact 5.5. Each of the following is true.

1. $+$ is a binary operation on $\mathbb{Z}$; that is, $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.
2. $\cdot$ is a binary operation on $\mathbb{Z}$; that is, $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.
3. $-$ is a binary operation on $\mathbb{Z}$; that is, $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.
4. $+$, $-$, and $\cdot$ are a binary operations on $\mathbb{Q}$.
5. $+$, $-$, and $\cdot$ are a binary operations on $\mathbb{R}$.
6. $\div$ is a binary operation on $\mathbb{Q} \setminus \{0\}$.
7. $\div$ is a binary operation on $\mathbb{R} \setminus \{0\}$.
8. $\cup$ is a binary operation on $\mathcal{P}(S)$.
9. $\cap$ is a binary operation on $\mathcal{P}(S)$.
10. $\setminus$ is a binary operation on $\mathcal{P}(S)$.

Before investigating properties of binary operations, one more example is needed. As we will see, this example has some very interesting properties and will be extremely important in later mathematics courses.

Definition 5.6. If A is a nonempty set,

$$\mathcal{S}(A) = \{f : A \to A \mid f \text{ is a bijection}\}$$

is called the ***symmetric group*** on A. The elements of $\mathcal{S}(A)$ are called ***permutations*** of A. In the special case where $A = \{1, 2, \ldots, n\}$, $\mathcal{S}(A)$ is denoted S_n.

Fact 5.7. $\circ$ is a binary operation on $\mathcal{F}(A)$ and on $\mathcal{S}(A)$.

Proof. Surely any two functions from A to A can be composed and will yield a function from A to A, so the range and domain of $\circ$ are appropriate. Let $f, g, h, k \in \mathcal{F}(A)$ with $f = h$ and $g = k$, which means $f(x) = h(x)$ and $g(x) = k(x)$ for all $x \in A$. Surely then, for any $x \in A$, we have $(g \circ f)(x) = g(f(x)) = g(h(x)) = k(h(x)) = (k \circ h)(x)$. Hence, equals composed with equals are equal and we can conclude $\circ$ is a binary operation on $\mathcal{F}(A)$.

Since Theorem 4.29 assures us that the composition of bijections from A to A is a bijection from A to A, we can conclude $\circ$ is a binary operation on $\mathcal{S}(A)$. $\square$

in class.

Defining Permutations in S_n.

Ex) To define a function $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, you can just specify what 1 maps to, what 2 maps to, etc.

f
$1 \to 3$
$2 \to 2$
$3 \to 1$
$4 \to 1$

Double line notation

$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$

$f \in S_4$ in general if $f \in S_n$, write

$f = \begin{pmatrix} 1, & 2, & \ldots, & n \\ f(1), & f(2), & \ldots, & f(n) \end{pmatrix}$

Composing Permutations

consider $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 5 & 6 \end{pmatrix} \in S_6$ and $g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 2 & 6 & 5 \end{pmatrix} \in S_6$

$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix} \in S_6$ $g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix} \in S_6$

Inverse of permutations:

Just swap rows!

$f : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix} \in S_5 \to f^{-1} = \begin{pmatrix} 5 & 4 & 2 & 1 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

Check: Using $f=\begin{pmatrix}1&2&3&4&5\\5&4&2&1&3\end{pmatrix} \to f^{-1}=\begin{pmatrix}5&4&2&1&3\\1&2&3&4&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\4&3&5&2&1\end{pmatrix} \to$ Now $f \circ f^{-1}=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}=I_5$

Cycles: $f \in S_n$ is a cycle if it acts like this: for some $a \in \{1,2,\dots,n\}$,

$$a \xrightarrow{f} f(a) \xrightarrow{f} f^2(a) \xrightarrow{f} f^3(a) \xrightarrow{f} \dots \xrightarrow{f} f^{(k-1)}(a) \xrightarrow{f} a$$

and "fixes" all elements not in the chain.

Ex| Consider $f=\begin{pmatrix}1&2&3&4&5&6&7\\1&4&3&6&5&7&2\end{pmatrix} \in S_7$

Notation: $f=(2,4,6,7) \in S_7$

Let $g=(4,1,3,8,6) \in S_9 \to g(4)=1,\ g(1)=3,\ g(3)=8$

Def: 2 cycles $f=(a_1,a_2,a_3,\dots,a_n)$ and $g=(b_1,b_2,\dots,b_n) \in S_n$ are disjoint if $A \cap B=\emptyset$

Theorem 5.14. *If $f=(a_1,a_2,\ldots,a_k)$ and $g=(b_1,b_2,\ldots,b_m)$ are disjoint cycles in S_n, then $f \circ g = g \circ f$. That is, disjoint cycles commute.*

Theorem 5.15. *Every permutation in S_n can be expressed as a product of disjoint cycles.*

Ex| Let

$$f=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12&13&14\\1&5&4&3&8&7&6&2&9&14&12&13&10&11\end{pmatrix} \in S_{14}.$$

$\to \cancel{(1)}(2,5,8),(3,4),(6,7),\cancel{(9)},(10,14,11,13)$

$$(3,2)\circ(4,2,1,9,7)\circ(6,5,4)\circ(9,5,6,7)\circ(1,3,5,9,4)=(1,2)\circ(3,5)\circ(4,9,6).$$

Chapter 6

Def: Let $x,y,z \in \mathbb{Z}$, $x \neq 0$. If $\exists\, n \in \mathbb{Z}$ with $y=x\cdot n$, we say x <u>divides</u> y or y is a multiple of x.

Notation: $x|y$.

If $x|y$ and $x|z$, we say x is a common divisor of y and z.

If $x|z$ and $y|z$, we say z is a common multiple of x and y.

Let $f: A \to B$ with $T_1, T_2 \subseteq B$

$f^{-1}(T_1 \setminus T_2) = f^{-1}(T_1) \setminus f^{-1}(T_2)$.

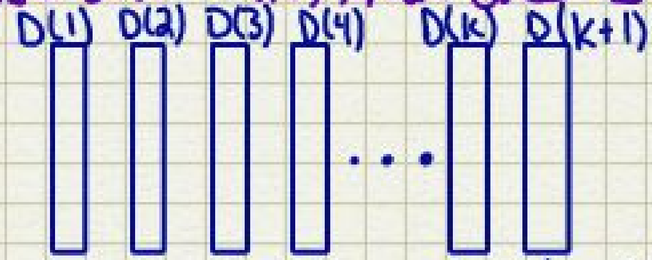
Proof:

($\subseteq$) Let $a \in f^{-1}(T_1 \setminus T_2)$. $\Rightarrow \exists\, t \in (T_1 \setminus T_2)$ s.t. $(a,t) \in f$.

$t \in T_1 \setminus T_2 \to t \in T_1 \land t \notin T_2$.

Chapter 6.2: Mathematical Induction

Def: Propositional functions are expressions $P(n)$ that are statements for particular values of n.



Ex| $P(n) = "n^2 > 8" \to P(1) = F \quad P(2) = F \quad P(3) = T$

suppose these dominoes have the ① property that for $k \in \mathbb{N}$ if $D(k)$ falls, $D(k+1)$ falls down. ② $D(1)$ falls down.

Ex| Let $P(n)$ be the sentence "$1+2+3+\cdots+n = \frac{n(n+1)}{2}$" } Want to Prove.

Axiom: (Well Ordering Principle): $(\mathbb{N}, \leq)$ is a well-ordered set. Every subset $B \subseteq \mathbb{N}$ has a minimum element.

First Principle of Mathematical Induction

Let $P(n)$ be a statement for each $n \in \mathbb{Z}$ with $n \geq 1$. If:

1. $P(1)$ is true and — base case
2. $P(k)$ being true implies $P(k+1)$ is true for $k \geq 1$ — $\underbrace{P(k)}_{\text{assume - Inductive Hypothesis}} \to P(k+1)$

then $P(n)$ is true for all $n \in \mathbb{Z}$ with $n \geq 1$. Inductive Step

The second Principle of Mathematical Induction

AKA "Strong Induction"

Let $P(n)$ be a propositional function with $n \in \mathbb{Z}$, $n \geq 1$.

If ① $P(1)$ is true, and

② The truth of $\underbrace{P(1), P(2), P(3), \cdots, \text{and } P(k-1)}_{\text{Inductive Hypotheses}}$ implies the truth of $P(k)$,

Then $P(n)$ is true for all $n \in \mathbb{Z}$, $n \geq 1$.

Ex| $24 \mid (2 \cdot 7^n + 3 \cdot 5^n - 5) \ \forall n \in \mathbb{N}$.

Proof by induction:

Base case: $n = 1 \to 14 + 15 - 5 = 24;\ 24 \mid 24$ ✓ Evidently true

Inductive step: Suppose $24 \mid (2 \cdot 7^m + 3 \cdot 5^m - 5)$ for $m \in \mathbb{Z}$, $1 \leq m < k$.

Consider $(2 \cdot 7^k + 3 \cdot 5^k - 5)$

6.2 Exercises

(e) $1^2-2^2+3^2-4^2\cdots=(-1)^{n-1}\dfrac{(n)(n+1)}{2}$

Base case

Let $n=1$

$(-1)^{(1-1)}=-1^0=1=1^2\checkmark$

$=\dfrac{1(2)}{2}=1$

Inductive step: (True for k) → (True for k+1)

Suppose $1^2-2^2+3^2-\cdots+n^2=(-1)^{n-1}\dfrac{(n(n+1))}{2}$

Then $1^2-2^2+3^2-\cdots+(-1)^{n-1}n^2+(-1)^{n-1}(n+1)^2=(-1)^{n-1}\left(\dfrac{n(n+1)}{2}\right)+(-1)^{(n+1-1)}(n+1)^2$

$=-1^{n-1}\left(\dfrac{n^2+n}{2}\right)+-1^n(n^2+2n+1)$

$=-1^n\left[(-1^{-1})\left(\dfrac{n^2+n}{2}\right)+(n^2+2n+1)\right]$

$=(-1^n)(-1^{-1})$

W.T.S.

$\dfrac{(-1)^{(n+1-1)}(n+1)(n+1+1)}{2}$

$=\dfrac{-1^n(n+1)(n+2)}{2}$

$(-1)^{k-1}=(-1)^k(-1)^{-1}$

$=-(-1)^k$

Prove $3\mid(n^3+2n)$

Base case → Let $n=1$

$3\mid(1^3+(2(1)))$

$3\mid(1+2)\checkmark$

Inductive

True for k → True for (k+1)

Let $3\mid(k^3+2k)$

Then $\exists\,\lambda\in\mathbb{Z}$ s.t. $(k^3+2k)=3\lambda$

$3\mid((k+1)^3+2(k+1))$

$\leftrightarrow 3\mid[(k^3+3k^2+3k+1)+(2k+2)]$

$3\mid k^3+3k^2+5k+3$

$k+1(k^2+2k+1)$

k^3+2k^2+k

$+k^2+2k+1$

k^3+3k^2+3k+1

Prove: For all integers $n \geq 1$, $1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$

Proof (by induction)

base case: $(n=1)$

If $n=1$, $1^2 = \frac{1(1+1)(2\cdot1+1)}{6}$ ✓

Inductive step: True for $k \to$ True for $(k+1)$

Let $k \geq 1 \in \mathbb{Z}$ and suppose that

$1^2+2^2+3^2+\cdots+k^2 = \frac{k(k+1)(2k+1)}{6}$. {W.T.S. $1^2+\cdots+(k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$}

Now $1^2+2^2+\cdots+(k+1)^2 = 1^2+\cdots+k^2+(k+1)^2$

$$= \frac{k(k+1)(2k+1)}{6}+(k+1)^2$$

$$= \frac{(k+1)[k(2k+1)+6(k+1)]}{6}$$

$$= \frac{(k+1)[2k^2+k+6k+6]}{6}$$

$$= \frac{(k+1)[2k^2+7k+6]}{6}$$

$$= \frac{(k+1)(k+2)(2k+3)}{6} = \frac{(k+1)[(k+1)+1][2(k+1)+1]}{6}$$

so by FPMI, $1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}$ $\forall n \in \mathbb{N}$ ■

$P(n) = f_n = \frac{(1+\sqrt{5})^n-(1-\sqrt{5})^n}{2^n\sqrt{5}}$

Sup. $P(m)$ is true for base $\leq m < k$ (WTS) $P(k)$

$f_k =$

base $\leq \underbrace{k-2 < k-1}_{m} < k$

Comprehensive Final: induction Set Equality
binary oper.

3 or 4 Proofs properties o' relations
- sym, trans, reflexive

Short Answer

image of union = union of images

"Compound" proofs $(p \to q) \leftrightarrow (\sim q \to \sim p)$

more second half than first

Prove n^2 even $\to$ n even

Suppose n is odd $\to$ n^2 odd

assume n^2 is even and n is odd. Then $(2k+1)$

$4k^2+4k+1 \to 2(2k^2+2k)+1$ odd.

$b^2 | a^2 \to b | a$

$b \nmid a \to b^2 \nmid a^2$