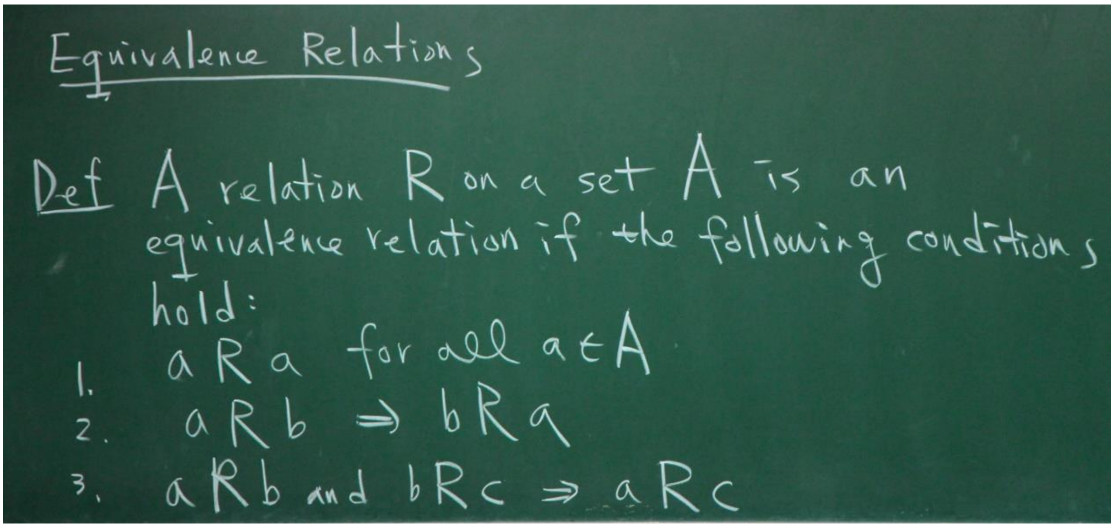
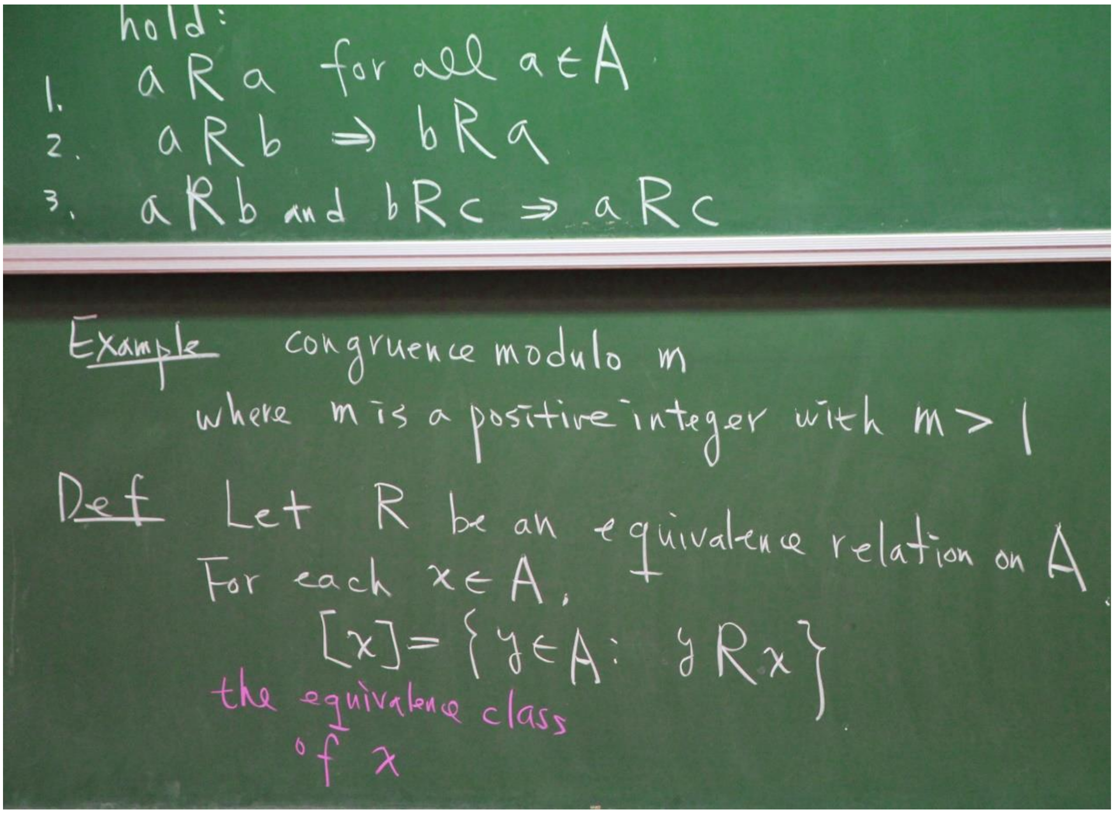
【10920 趙啟超教授離散數學 / 第 7 堂版書】



Equivalence Relations

Def A relation R on a set A is an equivalence relation if the following conditions hold:

1. aRa for all $a \in A$
2. $aRb \Rightarrow bRa$
3. aRb and $bRc \Rightarrow aRc$



hold:

1. aRa for all $a \in A$
2. $aRb \Rightarrow bRa$
3. aRb and $bRc \Rightarrow aRc$

Example congruence modulo m where m is a positive integer with $m > 1$

Def Let R be an equivalence relation on A. For each $x \in A$,

$$[x] = \{y \in A : yRx\}$$

the equivalence class of x

Equivalence Relations

Def A relation R on a set A is an equivalence relation if the following conditions hold:

1. aRa for all $a \in A$
2. $aRb \Rightarrow bRa$
3. aRb and $bRc \Rightarrow aRc$

Example congruence modulo m
where m is a positive integer with $m > 1$

Def Let R be an equivalence relation on A.
For each $x \in A$,

$$[x] = \{ y \in A : yRx \}.$$

the equivalence class of x

Property

1. $x \in [x]$.
2. xRy iff $[x] = [y]$
3. $[x] = [y]$ or $[x] \cap [y] = \phi$.

Proof 1. Since xRx (since R is reflexive)
$x \in [x]$.

$x \in [x]$.

$x R y$ iff $[x]=[y]$

$[x]=[y]$ or $[x] \cap [y] = \phi$.

1. Since $x R x$ (since R is reflexive)
   $x \in [x]$.

2. "$\Longrightarrow$" If $x R y$, let $w \in [x]$.
   Then $w R x$ and hence $w R y$ (since R is transitive)
   We have $w \in [y]$. Therefore, $\underline{[x] \subseteq [y]}$.
   If $t \in [y]$, then $t R y$.
   As $y R x$ (since R is symmetric) we have $t R x$.
   Hence $t \in [x]$. Therefore, $\underline{[y] \subseteq [x]}$.

<u>Property</u>

1. $x \in [x]$.
2. $x R y$ iff $[x]=[y]$
3. $[x]=[y]$ or $[x] \cap [y] = \phi$.

<u>Proof</u>

1. Since $x R x$ (since R is reflexive)
   $x \in [x]$.

2. "$\Longrightarrow$" If $x R y$, let $w \in [x]$.
   Then $w R x$ and hence $w R y$ (since R is transitive)
   We have $w \in [y]$. Therefore, $\underline{[x] \subseteq [y]}$.
   If $t \in [y]$, then $t R y$.
   As $y R x$ (since R is symmetric) we have $t R x$.
   Hence $t \in [x]$. Therefore, $\underline{[y] \subseteq [x]}$.

$\therefore [x] = [y]$.

"$\Longleftarrow$" Suppose $[x]=[y]$. Since $x \in [x]$, $x \in [y]$ and hence $x R y$.

3. If $x R y$, from part 2, $[x]=[y]$.
If $x \not R y$, let $[x] \cap [y] \neq \phi$.
There exists v such that $v \in [x]$ and $v \in [y]$.

$\therefore [x] = [y]$.

"$\Longleftarrow$" Suppose $[x]=[y]$. Since $x \in [x]$, $x \in [y]$ and hence $x R y$.

3. If $x R y$, from part 2, $[x]=[y]$.
If $x \not R y$, let $[x] \cap [y] \neq \phi$.
There exists v such that $v \in [x]$ and $v \in [y]$.

$x \in [y]$ and hence $x R y$.

3. If $x R y$, from part 2, $[x]=[y]$.
If $x \not R y$, let $[x] \cap [y] \neq \phi$.
There exists v such that $v \in [x]$ and $v \in [y]$.

We have $v R x$ and $v R y$.
Hence $x R v$ and $v R y$, which implies that $x R y$, contradicting the assumption that $x \not R y$. Therefore, we must have $[x] \cap [y] = \phi$. ∎

$\therefore\ [x] = [y].$

"$\Longleftarrow$" Suppose $[x]=[y]$. Since $x \in [x]$, $x \in [y]$ and hence $x R y$.

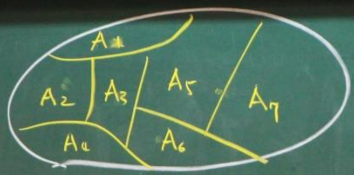
3. If $x R y$, from part 2, $[x]=[y]$.
If $x \not R y$, let $[x] \cap [y] \neq \phi$.
There exists v such that $v \in [x]$ and $v \in [y]$.
We have $v R x$ and $v R y$.
Hence $x R v$ and $v R y$, which implies that $x R y$, contradicting the assumption that $x \not R y$. Therefore, we must have $[x] \cap [y] = \phi$. ∎

Def A <u>partition</u> of a set A is a family $\{A_i : i \in I\}$ of nonempty subsets of A such that

1. $A = \bigcup_{i \in I} A_i$
2. $A_i \cap A_j = \phi$ for all $i \neq j$, $i, j \in I$.

such that

1. $A = \bigcup_{i \in I} A_i$
2. $A_i \cap A_j = \phi$ for all $i \neq j$, $i, j \in I$.



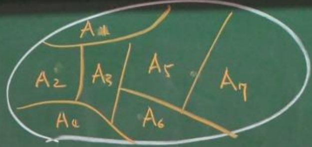
A

Property If R is an equivalence relation on a set A, then the distinct equivalence classes (with respect to R) form a partition of A.

Def A partition of a set A is a family $\{A_i : i \in I\}$ of nonempty subsets of A

such that

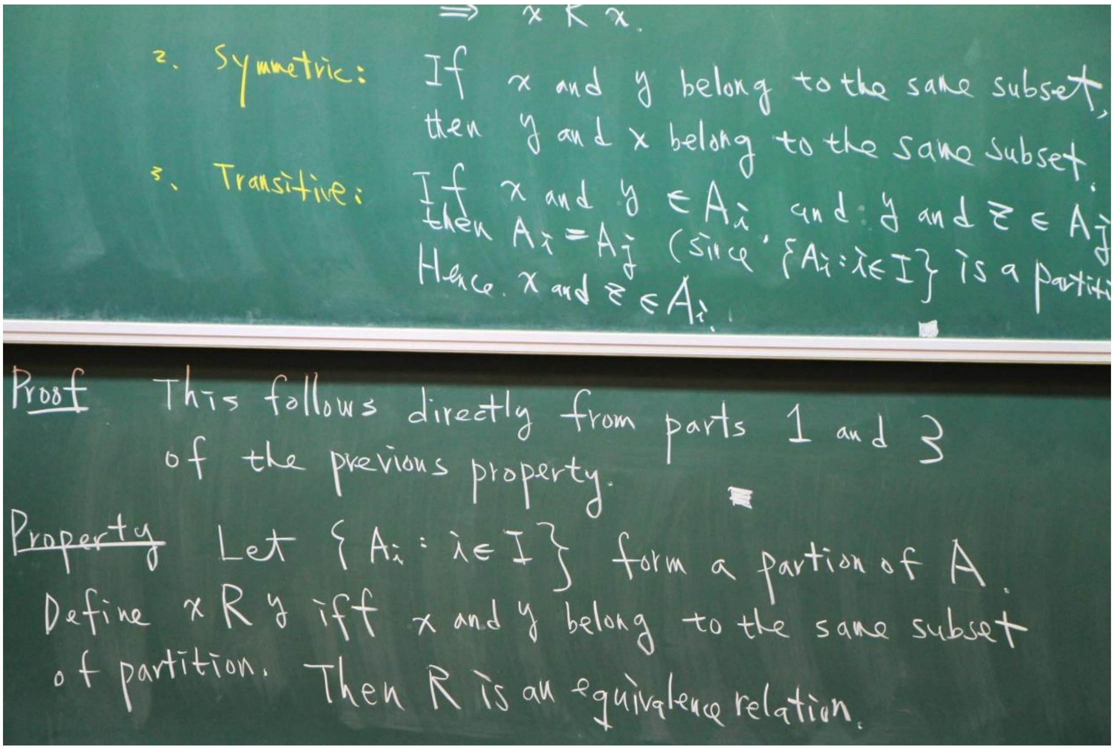
1. $A = \bigcup_{i \in I} A_i$
2. $A_i \cap A_j = \phi$ for all $i \neq j$, $i, j \in I$.

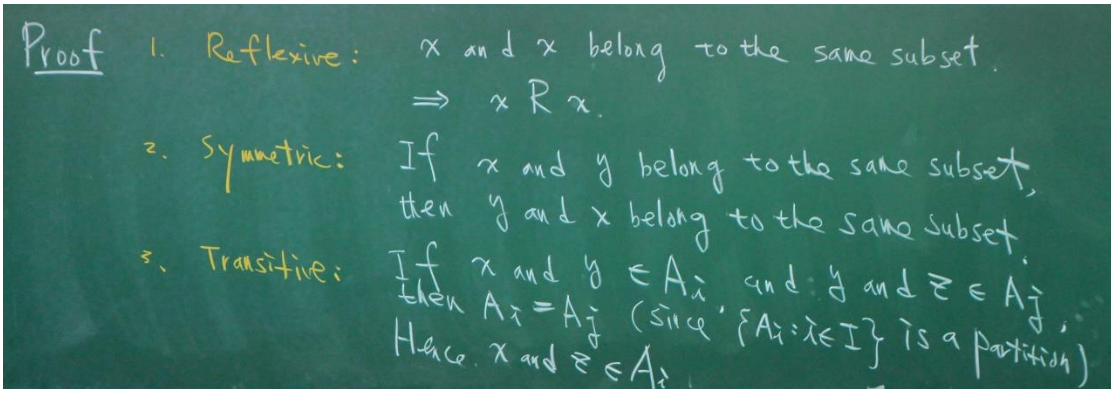


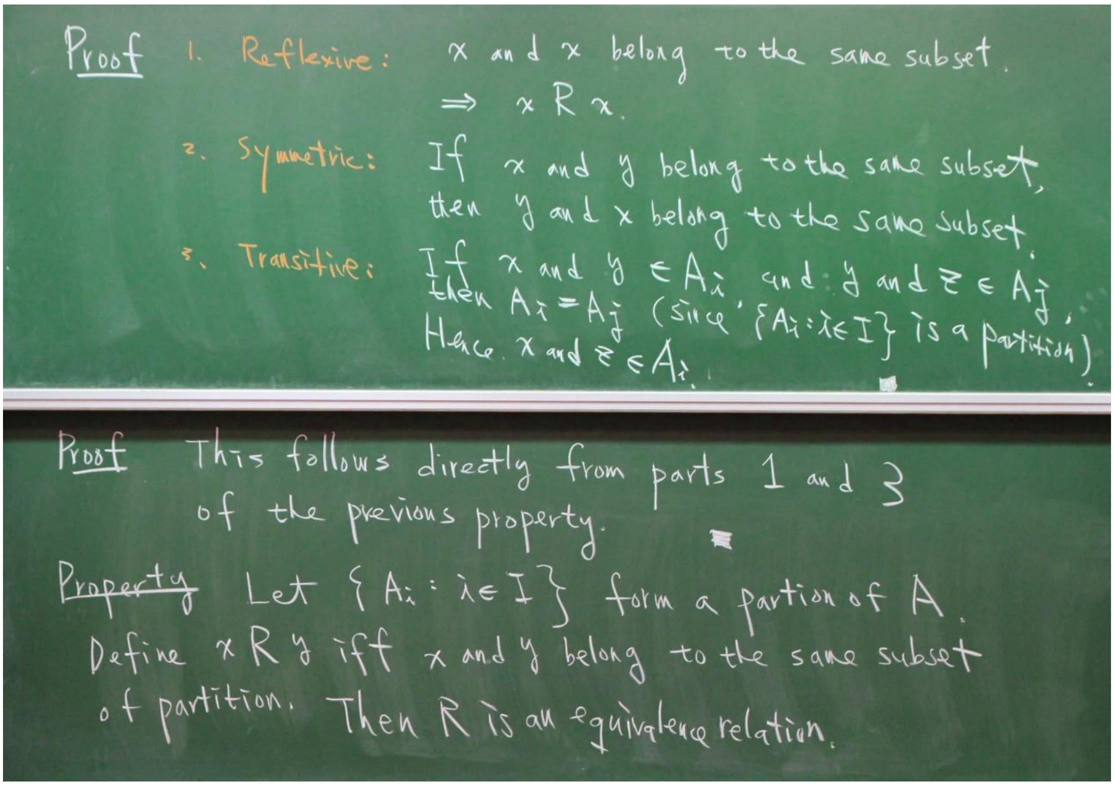
A

Property If R is an equivalence relation on a set A, then the distinct equivalence classes (with respect to R) form a partition of A.


2. $A_i \cap A_j = \phi$ for all $i \neq j$, $i, j \in I$.
A_1
A_2
A_3
A_5
A_7
A_4
A_6
A
Property If R is an
lation on
then the distinct
es (with
R) form a partit


$\Rightarrow x R x$.
2. Symmetric: If x and y belong to the same subset, then y and x belong to the same subset.
3. Transitive: If x and $y \in A_i$ and y and $z \in A_j$ then $A_i = A_j$ (since $\{A_i : i \in I\}$ is a partiti
Hence x and $z \in A_i$.
Proof This follows directly from parts 1 and 3 of the previous property.
Property Let $\{A_i : i \in I\}$ form a partion of A. Define $x R y$ iff x and y belong to the same subset of partition. Then R is an equivalence relation.


Proof 1. Reflexive: x and x belong to the same subset.
$\Rightarrow x R x$.
2. Symmetric: If x and y belong to the same subset, then y and x belong to the same subset.
3. Transitive: If x and $y \in A_i$ and y and $z \in A_j$, then $A_i = A_j$ (since $\{A_i : i \in I\}$ is a partition)
Hence x and $z \in A_i$


Proof 1. Reflexive: x and x belong to the same subset.
$\Rightarrow x R x$.
2. Symmetric: If x and y belong to the same subset, then y and x belong to the same subset.
3. Transitive: If x and $y \in A_i$ and y and $z \in A_j$, then $A_i = A_j$ (since $\{A_i : i \in I\}$ is a partition)
Hence x and $z \in A_i$.
Proof This follows directly from parts 1 and 3 of the previous property.
Property Let $\{A_i : i \in I\}$ form a partion of A.
Define $x R y$ iff x and y belong to the same subset of partition. Then R is an equivalence relation.

Hence $x R z$ and $z R y$, which implies that $x R y$, contradicting the assumption that $x \not R y$. Therefore, we must have $[x] \cap [y] = \phi$.

<u>Remark</u> For any set A, there is a one-to-one correspondence (bijection) between the set of equivalence relations on A and the set of partitions of A.

<u>Example</u> Congruence modulo m on $\mathbb{Z}$:

Each integer is congruent modulo m to one and only one of $0, 1, 2, \ldots, m-1$.

$$[0] = \{ \ldots, -2m, -m, 0, m, 2m, \ldots \}$$
$$[1] = \{ \ldots, -2m+1, -m+1, 1, m+1, 2m+1, \ldots \}$$
$$[2] = \{ \ldots, -2m+2, -m+2, 2, m+2, 2m+2, \ldots \}$$
$$\vdots$$
$$[m-1] = \{ \ldots, -m-1, -1, m-1, 2m-1, 3m-1, \ldots \}$$

<u>Example</u> Congruence modulo m on $\mathbb{Z}$:

Each integer is congruent modulo m to one and only one of $0, 1, 2, \ldots, m-1$.

$$[0] = \{ \ldots, -2m, -m, 0, m, 2m, \ldots \}$$
$$[1] = \{ \ldots, -2m+1, -m+1, 1, m+1, 2m+1, \ldots \}$$
$$[2] = \{ \ldots, -2m+2, -m+2, 2, m+2, 2m+2, \ldots \}$$
$$\vdots$$
$$[m-1] = \{ \ldots, -m-1, -1, m-1, 2m-1, 3m-1, \ldots \}$$

Example "$=$" is an equivalence relation.

equlity

$$[x] = \{x\}$$

singleton

Example "$=$" is an equivalence relation.

equlity

$$[x] = \{x\}$$

singleton

Partial Orders

Def A relation R on a set is a partial order (or a partial ordering relation) if the following conditions hold:

1. aRa for all $a \in A$ (reflexive)
2. aRb and $bRa \Rightarrow a = b$ (antisymmetric)
3. aRb and $bRc \Rightarrow aRc$ (transitive)

Example "$=$" is an equivalence relation.

equlity

$$[x] = \{x\}$$

singleton

Partial Orders

Def A relation R on a set is a partial order (or a partial ordering relation) if the following conditions hold:

1. $a \, R \, a$ for all $a \in A$ (reflexive)
2. $a R b$ and $b R a \Rightarrow a = b$ (antisymmetric)
3. $a R b$ and $b R c \Rightarrow a R c$ (transitive)

Example $A = \mathbb{N}$

$$a \, R \, b \Leftrightarrow a \mid b$$

Is "$\mid$" a partial order?

1. Reflexive: $a \mid a$ for all $a \in \mathbb{N}$
2. Antisymmetric: If $a \mid b$ and $b \mid a$, then

b/a and a/b are both positive integers

and $(b/a)^{-1} = a/b$ $\therefore$ $a/b = 1$

$\Rightarrow$ $a = b$.

3. Transitive: If $a|b$ and $b|c$, then

$b = ak_1$ and $c = bk_2$ for some $k_1, k_2 \in \mathbb{N}$

Hence $c = a(k_1 k_2)$, implying that $a|c$.

$\therefore$ "$|$" is a partial order.

Example $A = \mathbb{N}$

$a R b \Leftrightarrow a|b$

Is "$|$" a partial order?

1. Reflexive: $a|a$ for all $a \in \mathbb{N}$.

2. Antisymmetric: If $a|b$ and $b|a$, then

b/a and a/b are both positive integers

and $(b/a)^{-1} = a/b$ $\therefore$ $a/b = 1$

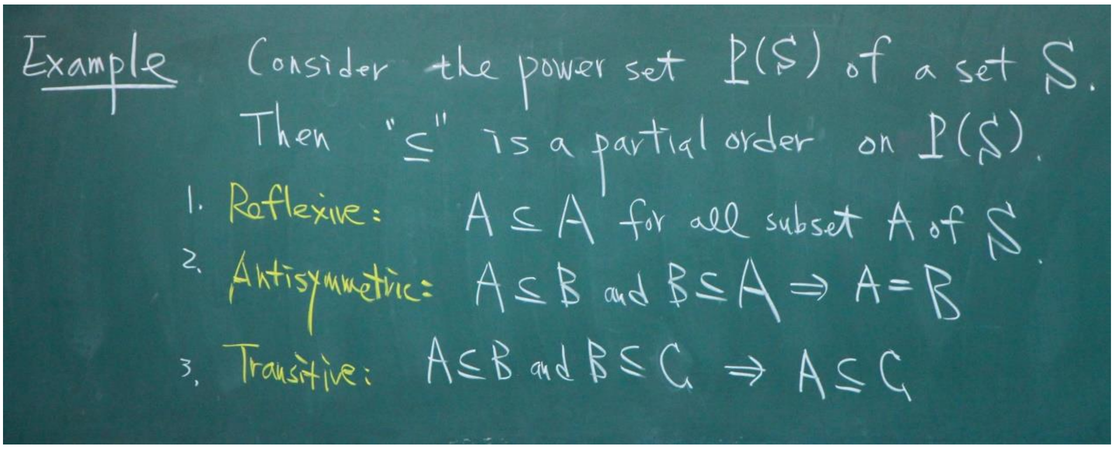
$\Rightarrow$ $a = b$.

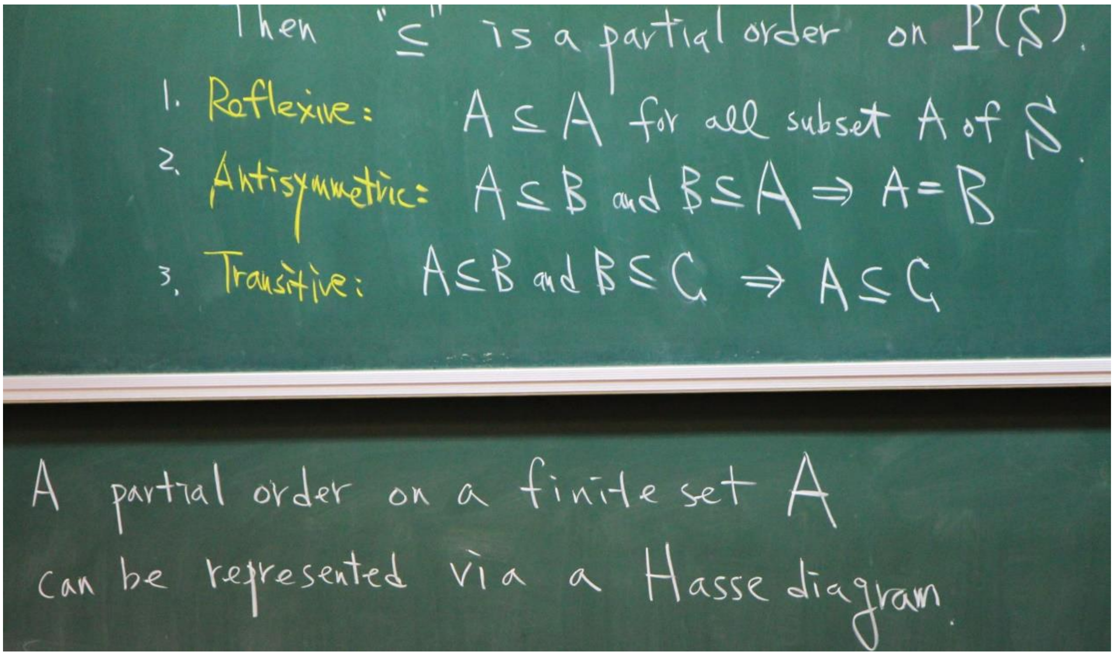
3. Transitive: If $a|b$ and $b|c$, then

$b = ak_1$ and $c = bk_2$ for some $k_1, k_2 \in \mathbb{N}$

Hence $c = a(k_1 k_2)$, implying that $a|c$.

$\therefore$ "$|$" is a partial order.


Example Consider the power set $P(S)$ of a set S.
Then "$\subseteq$" is a partial order on $P(S)$.
1. Reflexive: $A \subseteq A$ for all subset A of S.
2. Antisymmetric: $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$
3. Transitive: $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$


Then "$\subseteq$" is a partial order on $P(S)$.
1. Reflexive: $A \subseteq A$ for all subset A of S.
2. Antisymmetric: $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$
3. Transitive: $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$
A partial order on a finite set A
can be represented via a Hasse diagram.

Example Consider the power set $P(S)$ of a set S.
Then "$\subseteq$" is a partial order on $P(S)$.

1. Reflexive: $A \subseteq A$ for all subset A of S.
2. Antisymmetric: $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$
3. Transitive: $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$

A partial order on a finite set A can be represented via a Hasse diagram.

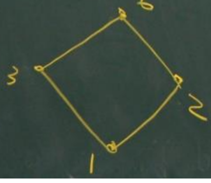
Suppose the partial order is "$\preceq$".
Each element of A is represented by a point, and we connect a to b (with a below b) with a line iff $a \prec b$, i.e. $a \preceq b$ and $a \neq b$, and there is no $c \in A$ such that $a \prec c \prec b$.

Each element of A is represented by a point,
and we connect a to b (with a below b)
with a line iff $a \prec b$, i.e., $a \preceq b$ and $a \neq b$,
and there is no $c \in A$ such that $a \prec c \prec b$.

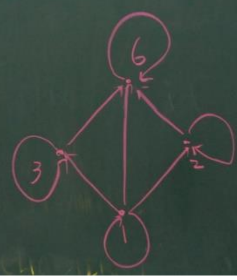
Example $A = \{ a \in \mathbb{N} : a \mid 6 \}$

$= \{1, 2, 3, 6\}$.

partial order: $\mid$



Hasse diagram



digraph

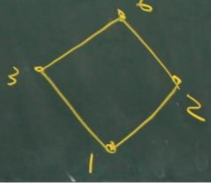
Suppose the partial order is "$\preceq$".

Each element of A is represented by a point,
and we connect a to b (with a below b)
with a line iff $a \prec b$, i.e., $a \preceq b$ and $a \neq b$,
and there is no $c \in A$ such that $a \prec c \prec b$.

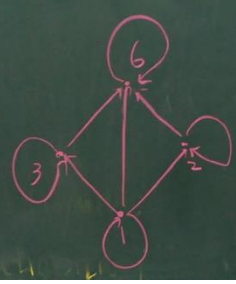
Example $A = \{ a \in \mathbb{N} : a \mid 6 \}$

$= \{1, 2, 3, 6\}$.

partial order: $\mid$



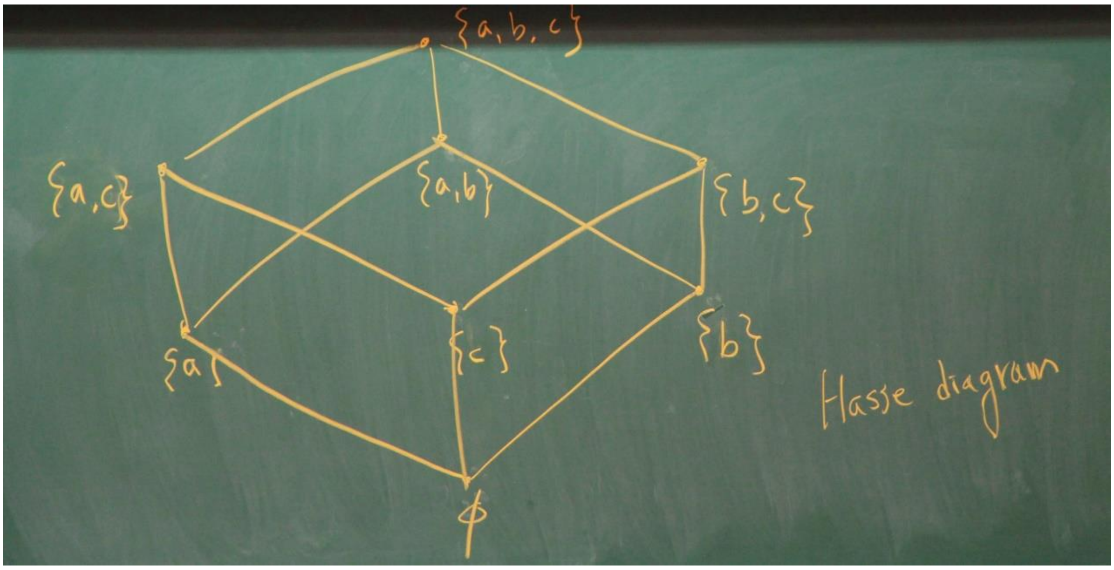
Hasse diagram



digraph

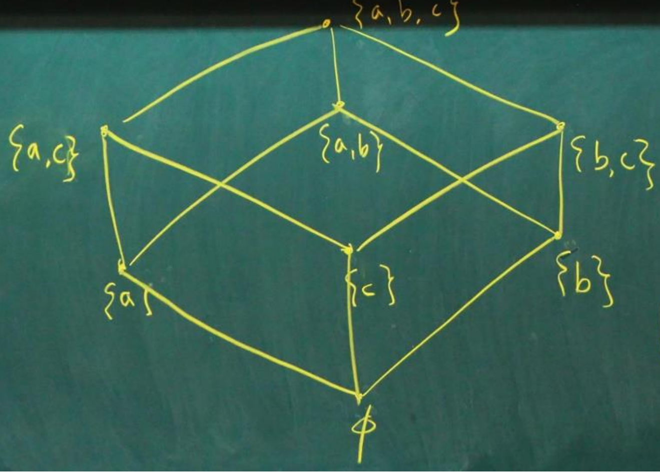
Example $A = \underline{P}(S)$ where $S = \{a, b, c\}$

partial order: $\subseteq$



Example $A = \underline{P}(S)$ where $S = \{a, b, c\}$

partial order: $\subseteq$



Hasse diagram