## Relations

> CSE 215: Foundations of Computer Science
> Stony Brook University

http:/ / www.cs.stonybrook.edu/~liu/ cse215

## Relations on sets

- $A$ (binary) relation $R$ from $A$ to $B$ is a subset of $A \times B$ (Section 1.3) For $(x, y) \in A \times B$, $x$ is related to $y$ by $R$ if, and only if, $(x, y) \in R$. $R$ is a subset of all pairs $(x, y), x$ in $A, y$ in $B . ~ x R y \Leftrightarrow(x, y) \in R$
- Example:

A less-than relation on real numbers: relation $L$ from $\mathbf{R}$ to $\mathbf{R}$ : for all x and y in $\mathbf{R}, \mathrm{x} L \mathrm{y} \Leftrightarrow \mathrm{x}<\mathrm{y}$
Examples: $(-17) \mathrm{L}(-14), \quad(-17) \mathrm{L}(-10), \quad(-35) \mathrm{L} 1$
The graph of L
as a subset of Cartesian plane $\mathbf{R} \times \mathbf{R}$ : It includes all points $(\mathrm{x}, \mathrm{y})$ with $\mathrm{y}>\mathrm{x}$, that is, all points above the line $\mathrm{x}=\mathrm{y}$.

## Relations: example 1

- The congruence modulo 2 relation:

Define relation $E$ from $\mathbf{Z}$ to $\mathbf{Z}$ : for all $(m, n) \in \mathbb{Z} \times \mathbf{Z}$,

$$
\mathrm{mEn} \Leftrightarrow m-\mathrm{n} \text { is even. }
$$

- Examples: 4 E 0 because $4-0=4$ and 4 is even.

2 E 6 because $2-6=-4$ and -4 is even.
$3 \mathrm{E}(-3)$ because $3-(-3)=6$ and 6 is even.

- Prove that if n is any odd integer, then n E 1 .

Proof: Suppose n is any odd integer.
Then $\mathrm{n}=2 \mathrm{k}+1$ for some integer k .
By definition of $E, n E 1 \Leftrightarrow n-1$ is even.
By substitution, $\mathrm{n}-1=(2 \mathrm{k}+1)-1=2 \mathrm{k}$.
3 Since k is an integer, 2 k is even. That is, $\mathrm{n}-1$ is even. Hence n E 1 .

## Relations: example 2

- A relation on a power set:
$X=\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}, \mathrm{P}(\mathrm{X})=\{\varnothing,\{\mathrm{a}\},\{\mathrm{b}\},\{\mathrm{c}\},\{\mathrm{a}, \mathrm{b}\},\{\mathrm{a}, \mathrm{c}\},\{\mathrm{b}, \mathrm{c}\},\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}\}$
Define relation S from $\mathrm{P}(\mathrm{X})$ to $\mathrm{P}(\mathrm{X})$ : $\quad$ (textbook says $\mathrm{P}(\mathrm{X})$ to Z ) for all sets $A$ and $B$ in $P(X)$,

ASB $\Leftrightarrow$ A has at least as many elements as $B$.

- Examples:
$\{\mathrm{a}, \mathrm{b}\} \mathrm{S}\{\mathrm{b}, \mathrm{c}\}$
$\{a\} S \emptyset$ because $\{a\}$ has one element, $\emptyset$ has zero elements, $1 \geq 0$.
\{c\} $S\{a\}$


## Inverse of a relation, and an example

- Let R be a relation from A to B.

The inverse relation $R^{-1}$ from $B$ to $A$ :

$$
R^{-1}=\{(y, x) \in B \times A \mid(x, y) \in R\}
$$

For all $x \in A, y \in B,(y, x) \in R^{-1} \Leftrightarrow(x, y) \in R$.

- Example: $A=\{2,3,4\}, B=\{2,6,8\}, R$ is the "divides" relation from A to B: for all $(x, y) \in A \times B, x R y \Leftrightarrow x \mid y$ ( $x$ divides $y$ ). $\mathrm{R}=\{(2,2),(2,6),(2,8),(3,6),(4,8)\} \quad \mathrm{R}^{-1}=\{(2,2),(6,2),(8,2),(6,3),(8,4)\}$


For all $(y, x) \in B \times A, y^{-1} x \Leftrightarrow y$ is a multiple of $x$.

## Inverse of a relation: example 2

- $R$ from $\mathbf{R}$ to $\mathbf{R}$ : for all $(\mathrm{x}, \mathrm{y}) \in \mathbf{R} \times \mathbf{R}, \mathrm{x} R \mathrm{y} \Leftrightarrow \mathrm{y}=2 \cdot|\mathrm{x}|$. $R$ and $R^{-1}$ in the Cartesian plane:

$R=$| $\{(x, y)\|y=2\| x \mid\}$ |  |
| ---: | ---: |
| $\boldsymbol{x}$ | $\boldsymbol{y}$ |
| 0 | 0 |
| 1 | 2 |
| -1 | 2 |
| 2 | 4 |
| -2 | 4 |
| 1st coordinate |  |





6 $R^{-1}$ is not a function because, for instance, both $(2,1)$ and $(2,-1)$ are in $R^{-1}$.

## Directed graph of a relation

- A relation on a set $\mathbf{A}$ is a relation from A to A .

Arrow diagram of the relation can be made into a directed graph.
For all points x and $\mathrm{y} \in \mathrm{A}$,
there is an arrow from x to $\mathrm{y} \Leftrightarrow \mathrm{x} \mathrm{R} \mathrm{y} \Leftrightarrow(\mathrm{x}, \mathrm{y}) \in \mathrm{R}$

- Example:

Let $A=\{3,4,5,6,7,8\}$.
Define relation R on A :

$$
\begin{aligned}
& \text { for all } \mathrm{x} \text { and } \mathrm{y} \in \mathrm{~A}, \\
& \mathrm{x} R \mathrm{y} \Leftrightarrow 2 \mid(\mathrm{x}-\mathrm{y})
\end{aligned}
$$



## N -ary relations and relational databases

- Given sets $A_{1}, A_{2}, \ldots, A_{n}$, an $\mathbf{n}$-ary relation $R$ on $A_{1} \times A_{2} \times \cdots A_{n}$ is a subset of $A_{1} \times A_{2} \times \cdots A_{n}$.
- Special cases: 2-ary, 3-ary, 4-ary, called binary, ternary, quaternary
- Example database: $\left(a_{1}, a_{2}, a_{3}, a_{4}\right) \in R \Leftrightarrow$ a patient with patient ID $a_{1}$, name $a_{2}$, was admitted on date $a_{3}$, with primary diagnosis $a_{4}$ Examples: (011985, John Schmidt, 120111, asthma) (244388, Sarah Wu, 010310, broken leg) (574329, Tak Kurosawa, 120111, pneumonia)


## In the database language SQL:

SELECT PatientID, Name FROM S WHERE AdmissionDate = 120111
011985 John Schmidt, 574329 Tak Kurosawa
setof((x.PatiendID, x.Name), x in S, x.AdmissionDate == 120111) da
$\{(x . P a t i e n t I D, x . N a m e)$ for $x$ in $S$ if $x . A d m i s s i o n D a t e==120111\} d a / p y$
8
\{(x.PatiendID, x.Name): x in S, x.AdmissionDate $=120111\}$

## Reflexivity, symmetry, and transitivity

- Properties of relations
- An example first:

Let $A=\{2,3,4,6,7,9\}$. Define a relation R on A:

$$
\text { for all } \mathrm{x} \text { and } \mathrm{y} \in \mathrm{~A}, \mathrm{x} R \mathrm{y} \Leftrightarrow 3 \mid(\mathrm{x}-\mathrm{y}) \text {. }
$$


$R$ is reflexive, symmetric, and transitive, to be defined next

## Reflexivity, symmetry, and transitivity

- Let R be a relation on a set A .

1. $R$ is reflexive iff for all $x \in A, x R x$, that is, $(x, x) \in R$
2. $R$ is symmetric iff for all $x, y \in A$, if $x R y$ then $y R x$
3. $R$ is transitive iff for all $x, y, z \in A$, if $x R y$ and $y R z$ then $x R z$

- Directed graph properties:

1. Reflexive: each point of the graph has a loop by itself.
2. Symmetric: whenever there is an arrow from one point to a second, there is an arrow from the second point back to the first.
3. Transitive: whenever there is an arrow from one point to a second and from the second point to a third, there is an arrow from the first point to the third.

## Reflexivity, symmetry, and transitivity: not

- R is not reflexive $\Leftrightarrow$
there is x in A such that $\mathrm{x} \not \subset \mathrm{x}$, that is, $(\mathrm{x}, \mathrm{x}) \notin \mathrm{R}$.
- R is not symmetric $\Leftrightarrow$ there are x and y in A such that $\mathrm{x} R \mathrm{y}$ but $\mathrm{y} R \mathrm{x}$, that is, $(x, y) \in R$ but $(y, x) \notin R$.
- R is not transitive $\Leftrightarrow$
there are $\mathrm{x}, \mathrm{y}$ and z in A such that $\mathrm{x} R \mathrm{y}$ and $\mathrm{y} R \mathrm{z}$ but $\mathrm{x} R \mathrm{z}$, that is, $(\mathrm{x}, \mathrm{y}) \in \mathrm{R}$ and $(\mathrm{y}, \mathrm{z}) \in \mathrm{R}$ but $(\mathrm{x}, \mathrm{z}) \notin \mathrm{R}$


## Properties of relations: example 1

- Let $A=\{0,1,2,3\}$.
$R=\{(0,0),(0,1),(0,3),(1,0),(1,1),(2,2),(3,0),(3,3)\}$

R is reflexive:
There is a loop at each point of the graph.
$R$ is symmetric: Whenever there is an arrow from one point of to a second,
 there is an arrow from the second point back to the first.
$R$ is not transitive: There is an arrow from 1 to 0 and
12) an arrow from 0 to 3 , but there is no arrow going from 1 to 3 .

## Properties of relations: example 2

- Let $A=\{0,1,2,3\}$.
$S=\{(0,0),(0,2),(0,3),(2,3)\}$

S is not reflexive:
There is no loop at 1.


S is not symmetric:
There is an arrow from 0 to 2 but not from 2 to 0 .

S is transitive!

## Properties of relations: example 3 <br> - Let $A=\{0,1,2,3\}$. <br> $\mathrm{T}=\{(0,1),(2,3)\}$ <br>  <br> $3 \bullet \longleftarrow \quad 2$

T is not reflexive:
There is no loop at 0 .

T is not symmetric:
There is an arrow from 0 to 1 but not from 1 to 0 .

T is transitive:
The transitivity condition is vacuously true for T .

## Properties of relations: example 4

- Equality relation on real numbers, an infinite set $R$ is a relation on real numbers, for all real numbers $x$ and $y$,

$$
x R y \Leftrightarrow x=y
$$

$R$ is reflexive: For all $x \in R, x R(x=x)$.
$R$ is symmetric: For all $x, y \in R$, if $x R y$ then $y R x$

$$
\text { (if } x=y \text { then } y=x \text { ). }
$$

$R$ is transitive: For all $x, y, z \in R$, if $x R y$ and $y R z$ then $x R z$

$$
\text { (if } \mathrm{x}=\mathrm{y} \text { and } \mathrm{y}=\mathrm{z} \text { then } \mathrm{x}=\mathrm{z} \text { ). }
$$

## Properties of relations: example 5

- Less-than relation: For all $x, y \in R, x R y \Leftrightarrow x<y$.
$R$ is not reflexive: $R$ is reflexive iff, $\forall \mathrm{x} \in \mathrm{R}, \mathrm{x} R \mathrm{x}$. By definition of $R$, this means that $\forall x \in R, x<x$. This is false: $\exists \mathrm{x}=0 \in \mathrm{R}$ such that $\mathrm{x} \nless \mathrm{x}$.
$R$ is not symmetric: $R$ is symmetric iff $\forall x, y \in R$, if $x R y$ then $y R x$ By definition of $R$, this means that $\forall x, y \in R$, if $x<y$ then $y<x$ This is false: $\exists \mathrm{x}=0, \mathrm{y}=1 \in \mathrm{R}$ such that $\mathrm{x}<\mathrm{y}$ and $\mathrm{y} \nless \mathrm{x}$.
$R$ is transitive: $R$ is transitive iff $\forall x, y, z \in R$, if $x R y, y R z$, then $x R z$ By definition of $R$, this means $\forall x, y, z \in R$, if $x<y, y<z$, then $x<z$


## Properties of relations: example 6

- Congruence modulo 3

$$
\text { For all } \mathrm{x} \text { and } \mathrm{y} \in \mathrm{Z}, \mathrm{~m} \operatorname{Tn} \Leftrightarrow 3 \mid(\mathrm{m}-\mathrm{n}) \text {. }
$$

T is reflexive: Suppose m is any integer. [We must show that $\mathrm{m} T \mathrm{~m}$.] $\mathrm{m}-\mathrm{m}=0$. And $3 \mid 0$ because $0=3 \cdot 0$.
Hence $3 \mid(\mathrm{m}-\mathrm{m})$. By definition of T, m T m
T is symmetric: Suppose m and n are integers that satisfy m Tn .
[We must show that $n T$ m.]
By definition of $\mathrm{T}, \mathrm{m} \mathrm{Tn}$ implies $3 \mid(\mathrm{m}-\mathrm{n})$.
By definition of "divides," $m-n=3 k$, for some integer $k$.
Multiplying both sides by -1 gives $n-m=3(-\mathrm{k})$.
Since $-k$ is an integer, this equation shows $3 \mid(n-m)$.
By definition of $\mathrm{T}, \mathrm{nT} \mathrm{m}$.

## Properties of relations: example 6 (II)

- Congruence modulo 3

$$
\text { For all } \mathrm{x}, \mathrm{y} \in \mathrm{Z}, \mathrm{mTn} \Leftrightarrow 3 \mid(\mathrm{m}-\mathrm{n}) \text {. }
$$

T is transitive: Suppose $m, n$, and $p$ are any integers that satisfy mTn and nT . [ We must show that $m T p$.]
By definition of $T, m T n$ and $n T p$ means $3 \mid(m-n)$ and $3 \mid(n-p)$. By definition of "divides," this means $\mathrm{m}-\mathrm{n}=3 \mathrm{r}$ and $\mathrm{n}-\mathrm{p}=3 \mathrm{~s}$, for some integers $r$ and $s$.
Adding the two equations gives $(\mathrm{m}-\mathrm{n})+(\mathrm{n}-\mathrm{p})=3 \mathrm{r}+3 \mathrm{~s}$, and simplifying gives that $\mathrm{m}-\mathrm{p}=3(\mathrm{r}+\mathrm{s})$.
Since $r+s$ is an integer, this equation shows $3 \mid(m-p)$.
18 By definition of T, m T p.

## The transitive closure of a relation

- Let A be a set and R a relation on A . The transitive closure of $\mathbf{R}$ is the relation $R^{t}$ on $A$ that satisfies the following three properties:

1. $\mathrm{R}^{\mathrm{t}}$ is transitive
2. $R \subseteq R^{t}$
3. If $S$ is any other transitive relation that contains $R$, then $R^{t} \subseteq S$

- Example:

$$
\begin{aligned}
\mathrm{A}= & \{0,1,2,3\} \\
\mathrm{R}= & \{(0,1),(1,2),(2,3)\} \\
\mathrm{R}^{\mathrm{t}}= & \{(0,1),(0,2),(0,3), \\
& (1,2),(1,3),(2,3)\}
\end{aligned}
$$



## Equivalence relations

- An example first: Given a partition of a set A (Section 6), the relation induced by the partition, R , is defined on A as follows: for all $\mathrm{x}, \mathrm{y} \in \mathrm{A}$,

$$
x R y \Leftrightarrow \exists \text { subset } A_{i} \text { of the partition, } x \in A_{i} \text { and } y \in A_{i} .
$$

- Example: A $=\{0,1,2,3,4\}$. Consider partition: $\{0,3,4\},\{1\},\{2\}$ 0 R 3 because both 0 and 3 are in $\{0,3,4\} \quad 3$ R 0 because both 3 and 0 are in $\{0,3,4\}$ 0 R 4 because both 0 and 4 are in $\{0,3,4\} \quad 4 \mathrm{R} 0$ because both 4 and 0 are in $\{0,3,4\}$ 3 R 4 because both 3 and 4 are in $\{0,3,4\} \quad 4 \mathrm{R} 3$ because both 4 and 3 are in $\{0,3,4\}$ 0 R 0 because both 0 and 0 are in $\{0,3,4\} \quad 3 R 3$ because both 3 and 3 are in $\{0,3,4\}$ 4 R 4 because both 4 and 4 are in $\{0,3,4\}$

1 R 1 because both 1 and 1 are in $\{1\} \quad 2$ R 2 because both 2 and 2 are in $\{2\}$
$R=\{(0,0),(0,3),(0,4),(1,1),(2,2),(3,0),(3,3),(3,4),(4,0),(4,3),(4,4)\}$

## Relation induced by a partition

- Let A be a set with a partition. Let R be the relation induced by the partition. Then R is reflexive, symmetric, and transitive.
Proof: for finite partition but same for infinite except for notation Suppose $A$ is a set with a partition $A_{1}, A_{2}, \ldots, A_{n}$,

$$
\mathrm{A}_{\mathrm{i}} \cap \mathrm{~A}_{\mathrm{j}}=\varnothing \text { whenever } \mathrm{i}^{\mathrm{i}}=\mathrm{j} \text {, and } \mathrm{A}_{1} \cup \mathrm{~A}_{2} \cup \cdots \cup \mathrm{~A}_{\mathrm{n}}=\mathrm{A} .
$$

For all $\mathrm{x}, \mathrm{y} \in \mathrm{A}, \mathrm{x} \mathrm{R} \mathrm{y} \Leftrightarrow \exists \operatorname{set} \mathrm{A}_{\mathrm{i}}$ in the partition, $\mathrm{x} \in \mathrm{A}_{\mathrm{i}}$ and $\mathrm{y} \in \mathrm{A}_{\mathrm{i}}$
(Reflexive) Suppose $x \in A$. Since $A_{1} \cup A_{2} \cup \cdots \cup A_{n}=A, x \in A_{i}$ for some i.
That is, $\exists \operatorname{set} A_{i}, x \in A_{i}$ and $x \in A_{i}$. By definition of $R, x R x$.
(Symmetric) Suppose x and y are in A and $\mathrm{x} R \mathrm{y}$.
Then by definition of $R, \exists \operatorname{set} A_{i}$ in the partition, $x \in A_{i}$ and $y \in A_{i}$. Then, $\exists \operatorname{set} A_{i}, y \in A_{i}$ and $x \in A_{i}$. By definition of $R, y R x$.

## Relation induced by a partition (II)

(Transitive) Suppose $\mathrm{x}, \mathrm{y}$, and z are in A and $\mathrm{x} R \mathrm{y}$ and y Rz .
Then by definition of $R, \exists$ sets $A_{i}$ and $A_{j}$ in the partition such that $x$ and $y$ are in $A_{i}$, and $y$ and $z$ are in $A_{j}$.

Suppose $A_{i} \neq A_{j}$. [We will deduce a contradiction.]
Then $A_{i} \cap A_{j}=\emptyset$ since $\left\{A_{1}, A_{2}, A_{3}, \ldots, A_{n}\right\}$ is a partition of $A$.
But $y$ is in $A_{i}$ and $y$ is in $A_{j}$. Thus $A_{i} \cap A_{j} \neq \emptyset$. Contradicts $A_{i} \cap A_{j}=\varnothing$.
Thus $\mathrm{A}_{\mathrm{i}}=\mathrm{A}_{\mathrm{j}}$.

So, $\mathrm{x}, \mathrm{y}$, and z are all in $\mathrm{A}_{\mathrm{i}}$.
That is, $\exists \operatorname{set} A_{i}, x \in A_{i}$ and $z \in A_{i}$. By definition of $R, x R z$.

## Equivalence relation

- Let A be a set, R be a relation on A . R is an equivalence relation if, and only if, $R$ is reflexive, symmetric, and transitive.
- Example: $\mathrm{X}=\{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$

ARB $\Leftrightarrow$ the least element of $A=$ the least element of $B$
Prove that R is an equivalence relation on X :
(Reflexive) Suppose A is a nonempty subset of $\{1,2,3\}$
The least element of $\mathrm{A}=$ the least element of A . By definition of $\mathrm{R}, \mathrm{ARA}$. (Symmetric) Suppose A and B are nonempty subsets of $\{1,2,3\}$ and A R B. By A R B, the least element of A = the least element of B .
By symmetry of equality, B R A.
(Transitive) Suppose A, B, C are nonempty subsets of $\{1,2,3\}$, A R B and B R C. By A R B, the least element of A = the least element of B. By B R C, the least element of $\mathrm{B}=$ the least element of C . By transitivity of equality, the least element of $\mathrm{A}=$ the least element of C. So A R C.

## Equivalence classes

- Let A be a set, R be an equivalence relation on A . For each a in A , the equivalence class of a (the class of a) is the set of all $x$ in $A$ such that x is related to a by $R$.

$$
[a]=\{x \in A \mid x R a\}
$$

- Example: Let $\mathrm{A}=\{0,1,2,3,4\}$, and R be a relation on A :

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

$R$ is an equivalence relation: check.
$[0]=\{x \in A \mid x R 0\}=\{0,4\} .[4]=$ same $[1]=\{x \in A \mid x R 1\}=\{1,3\} .[3]=$ same $[2]=\{x \in A \mid x R 2\}=\{2\}$

## Equivalence classes: example 2

- Equivalence classes of a relation on a set of subsets

$$
X=\{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}
$$

ARB $\Leftrightarrow$ the least element of $A=$ the least element of B
$R$ is an equivalence relations (proved 3 slides back)
$[\{1\}]=\{1\},\{1,2\},\{1,3\},\{1,2,3\}\}$.

$$
[\{1,2\}]=[\{1,3\}]=[\{1,2,3\}]=\text { same }
$$

$$
[\{2\}]=\{\{2\},\{2,3\}\} . \quad[\{2,3\}]=\text { same }
$$

$$
[\{3\}]=\{\{3\}\}
$$

## Equivalence classes: example 3

- Equivalence classes of the identity relation

Let A be any set. Let R be a relation on A : For all x and y in A ,

$$
x R y \Leftrightarrow x=y
$$

$R$ is an equivalence relation: easy to prove.

Given any a in A, the class of a is:

$$
[a]=\{x \in A \mid x R a\}=\{a\}
$$

because the only element of A that equals a is a.

## Equivalence classes: example proof 1

- Let A be a set, R be an equivalence relation on A , and a and b be elements of $A$. If a $R b$, then $[a]=[b]$.

Proof: $[\mathrm{a}]=[\mathrm{b}] \Leftrightarrow[\mathrm{a}] \subseteq[\mathrm{b}]$ and $[\mathrm{b}] \subseteq[\mathrm{a}]$.

1. Proof of $[\mathrm{a}] \subseteq[\mathrm{b}]$ :

Let $x \in[a]$. Then $x R$ a, by definition of [a].
a R b by hypothesis $\rightarrow$ by transitivity of $\mathrm{R}, \mathrm{xRb} \rightarrow \mathrm{x} \in[\mathrm{b}]$
2. Proof of $[\mathrm{b}] \subseteq[\mathrm{a}]$ :

Let $x \in[b]$. Then $x R b$, by definition of $[b]$.
b R a by hypothesis and symmetry $\boldsymbol{\rightarrow}$ by transitivity of $\mathrm{R}, \mathrm{x}$ R a $\rightarrow \mathrm{x} \in[\mathrm{a}]$

## Equivalence classes: example proof 2

- Let A be a set, R be an equivalence relation on A , and a and b are elements of A. Either $[\mathrm{a}] \cap[\mathrm{b}]=\varnothing$ or $[\mathrm{a}]=[\mathrm{b}]$.


## Proof:

Suppose A is a set, R is an equivalence relation on A , a and b are elements of A , and $[\mathrm{a}] \cap[\mathrm{b}] \neq \varnothing$. [We must show $[\mathrm{a}]=[\mathrm{b}]]$ Since $[a] \cap[b] \neq \emptyset, \exists \mathrm{x}$ in A such that $\mathrm{x} \in[\mathrm{a}] \cap[\mathrm{b}]$
$\rightarrow \mathrm{x} \in[\mathrm{a}]$ and $\mathrm{x} \in[\mathrm{b}] \rightarrow$ so xR a and xRb By symmetry and transitivity, $\mathrm{R} \mathrm{b} \rightarrow[\mathrm{a}]=[\mathrm{b}]$.

- If R is an equivalence relation on A , then the distinct equivalence classes of $R$ form a partition of $A$ : union of those classes is all of $A$, and intersection of any two distinct classes is empty.


## Equivalence classes: example 4

- Let R be the relation of congruence modulo $\mathbf{3}$ on $\mathbf{Z}$ :
for all m and n in $\mathbb{Z}, \mathrm{mRn} \Leftrightarrow 3 \mid(\mathrm{m}-\mathrm{n}) \Leftrightarrow \mathrm{m} \equiv \mathrm{n}(\bmod 3)$.
For each integer $a$,

$$
\begin{aligned}
{[a] } & =\{x \in Z|3|(x-a)\}=\{x \in Z \mid x-a=3 k, \text { for some integer } k\} \\
& =\{x \in Z \mid x=3 k+a, \text { for some integer } k\} .
\end{aligned}
$$

$$
[0]=\{x \in Z \mid x=3 k+0, \text { for some integer } k\}
$$

$$
=\{\ldots-9,-6,-3,0,3,6,9, \ldots\}=[3]=[-3]=[6]=[-6]=\ldots
$$

$[1]=\{x \in Z \mid x=3 k+1$, for some integer $k\}$

$$
=\{\ldots-8,-5,-2,1,4,7,10, \ldots\}=[4]=[-2]=[7]=[-5]=\ldots
$$

$[2]=\{x \in Z \mid x=3 k+2$, for some integer $k\}$

$$
=\{\ldots-7,-4,-1,2,5,8,11, \ldots\}=[5]=[-1]=[8]=[-4]=\ldots
$$

## Some terminologies

- Let R be an equivalence relation on a set $\mathrm{A}, \mathrm{S}$ be an equivalence class of $R$. A representative of the class $S$ is any element a in $A$ such that $[\mathrm{a}]=\mathrm{S}$.
- Let m and n be integers, and let d be a positive integer. $\mathbf{m}$ is congruent to $\mathbf{n}$ modulo $d, \mathbf{m} \equiv \mathbf{n}(\bmod \mathbf{d})$, iff $\mathrm{d} \mid(\mathrm{m}-\mathrm{n})$. That is,

$$
\mathrm{m} \equiv \mathrm{n}(\bmod \mathrm{~d}) \Leftrightarrow \mathrm{d} \mid(\mathrm{m}-\mathrm{n})
$$

Example:

$$
12 \equiv 7(\bmod 5) \text { because } 12-7=5=5 \cdot 1 \rightarrow 5 \mid(12-7)
$$

## Equivalence classes: example 6

- Rational numbers are equivalence classes

Let A be the set of all ordered pairs of integers for which the second element of the pair is nonzero: $A=Z \times(Z-\{0\})$
$R$ is a relation on $A$ : for all $(a, b),(c, d) \in A$,

$$
(a, b) R(c, d) \Leftrightarrow a d=b c \quad(a / b=c / d)
$$

$R$ is an equivalence relation.

Example:

$$
\begin{gathered}
{[(1,2)]=\{(1,2),(-1,-2),(2,4),(-2,-4),(3,6),(-3,-6), \ldots\}} \\
\frac{1}{2}=\frac{-1}{-2}=\frac{2}{4}=\frac{-2}{-4}=\frac{3}{6}=\frac{-3}{-6} \text { and so forth. }
\end{gathered}
$$

## Modular arithmetic

- Example: 12-hour analog clock

5 o'clock +10 hours: $(5+10) \bmod 12=15 \bmod 12=3$

- Properties of congruence modulo $n$, to do arithmetic modulo $n$.
- Equivalence classes of integers modulo $n$, and extend arithmetic to add and multiply such classes, $\mathbf{Z}_{\mathbf{n}}$
- Applications to cryptography: encrypt/decrypt messages. RSA: prime factors and modulo arithmetic.

Too hard to find large prime factors-hundreds of digits.

## Euclid algorithm and applications

- Euclid algorithm finding GCD

We've seen at the end of the topics on number theory (and even did extra-credit programing, a few lines)

- More proofs and uses

These use modular arithmetic.

## Partial order relations

- Antisymmetry

Let R be a relation on a set A .
$R$ is antisymmetric if, and only if, for all a and b in A , if $a R b$ and $b R a$, then $a=b$
$R$ is not antisymmetric $\Leftrightarrow$ there are $a$ and $b$ in $A$ such that
$\mathrm{a} R \mathrm{~b}$ and b R a but $\mathrm{a} \neq \mathrm{b}$


0 R 2 and 2 R 0 but $0 \neq 2$

## Antisymmetry: examples using "divides"

- Example 1: For all $a, b \in \mathbb{Z}^{+}, a R_{1} b \Leftrightarrow a \mid b$.
$\mathrm{R}_{1}$ is antisymmetric: Suppose $\mathrm{a}, \mathrm{b} \in \mathbf{Z}^{+}$has a $\mathrm{R}_{1} \mathrm{~b}$ and $\mathrm{b} \mathrm{R}_{1} \mathrm{a}$.
[We must show that $\mathrm{a}=\mathrm{b}$ ]
By definition of $\mathrm{R}_{1}, \mathrm{a} \mid \mathrm{b}$ and $\mathrm{b} \mid \mathrm{a} \rightarrow \mathrm{b}=\mathrm{k}_{1} \mathrm{a}$ and $\mathrm{a}=\mathrm{k}_{2} \mathrm{~b}$, for $\mathrm{k}_{1}, \mathrm{k}_{2} \in \mathrm{Z}$ $\rightarrow \mathrm{b}=\mathrm{k}_{1} \mathrm{k}_{2} \mathrm{~b}$
Dividing both sides by b gives $\mathrm{k}_{1} \mathrm{k}_{2}=1 \rightarrow \mathrm{k}_{1}=\mathrm{k}_{2}=1 \rightarrow \mathrm{a}=\mathrm{b}$
- Example 2: For all $a, b \in \mathbb{Z}, a R_{2} b \Leftrightarrow a \mid b$. $\mathrm{R}_{2}$ is not antisymmetric:
Counterexample: $\mathrm{a}=2$ and $\mathrm{b}=-2 \boldsymbol{\rightarrow} \mathrm{a} \neq \mathrm{b}$

$$
\begin{aligned}
& \mathrm{a} \mid \mathrm{b} \text { because }-2=(-1) \cdot 2 \rightarrow \mathrm{a}_{2} \mathrm{~b} \\
& \mathrm{~b} \mid \mathrm{a} \text { because } 2=(-1)(-2) \rightarrow \mathrm{bR}_{2} \mathrm{a}
\end{aligned}
$$

## Partial order relations

- Let R be a relation on a set A . R is a partial order relation if, and only if, R is reflexive, antisymmetric, and transitive.

> (no cycles besides self cycles)
> (partial order vs. total order)

- Example: The "Subset" ( $\subseteq$ ) relation on sets.

Let A be a set of sets. Define $\subseteq$ relation on A :
For all $U, V \in A, U \subseteq V \Leftrightarrow$ for all $x$, if $x \in U$ then $x \in V$.
$\subseteq$ is a partial order
Proof: (Antisymmetric) for all sets U and V in A , if $\mathrm{U} \subseteq \mathrm{V}$ and $\mathrm{V} \subseteq \mathrm{U}$ then $\mathrm{U}=\mathrm{V}$ (by definition of equality of sets)

## Partial order relations: example 2

- The "less than or equal to" $(\leq)$ relation on $\mathbf{R}$ : for all x and y in $\mathbf{R}, \mathrm{x} \leq \mathrm{y} \Leftrightarrow \mathrm{x}<\mathrm{y}$ or $\mathrm{x}=\mathrm{y}$.
$\leq$ is a partial order relation


## Proof:

(Reflexive) $\mathrm{x} \leq \mathrm{x}$ means that $\mathrm{x}<\mathrm{x}$ or $\mathrm{x}=\mathrm{x}$, and $\mathrm{x}=\mathrm{x}$ is true.
Thus $\mathrm{x} \leq \mathrm{x}$ for all real numbers.
(Antisymmetric) for all x and y in $\mathbf{R}$, if $\mathrm{x} \leq \mathrm{y}$ and $\mathrm{y} \leq \mathrm{x}$ then $\mathrm{x}=\mathrm{y}$.
(Transitive) for all $\mathrm{x}, \mathrm{y}$, and z in $\mathbf{R}$, if $\mathrm{x} \leq \mathrm{y}$ and $\mathrm{y} \leq \mathrm{z}$ then $\mathrm{x} \leq \mathrm{z}$.

## example 3: Lexicographic order

- Order in an English dictionary: compare letters one by one from left to right in words.
- Let A be a set (of letters, etc) with a partial order relation R.

Let $S$ be a set of strings over A. Define relation $\preccurlyeq$ on $S$ :
For any 2 strings in $S, a_{1} a_{2} \ldots a_{m}$ and $b_{1} b_{2} \ldots b_{n}$, where $m, n \in \mathbb{Z}^{+}$,

1. If $m \leq n$ and $a_{i}=b_{i}$ for all $i=1,2, \ldots, m$, then $a_{1} a_{2} \ldots a_{m} \leqslant b_{1} b_{2} \ldots b_{n}$
2. If for some integer k with $\mathrm{k} \leq \mathrm{m}, \mathrm{k} \leq \mathrm{n}$, and $\mathrm{k} \geq 1, \mathrm{a}_{\mathrm{i}}=\mathrm{b}_{\mathrm{i}}$ for all
$\mathrm{i}=1,2, \ldots, \mathrm{k}-1$, and $\mathrm{a}_{\mathrm{k}} \neq \mathrm{b}_{\mathrm{k}}$, but $\mathrm{a}_{\mathrm{k}} R \mathrm{~b}_{\mathrm{k}}$ then $\mathrm{a}_{1} \mathrm{a}_{2} \ldots \mathrm{a}_{\mathrm{m}} \preccurlyeq \mathrm{b}_{1} \mathrm{~b}_{2} \ldots \mathrm{~b}_{\mathrm{n}}$.
3. If $\varepsilon$ is the null string, and $s$ is any string in $S$, then $\varepsilon \preccurlyeq s$.
(messy, complex cases)
If no strings are related other than by these three conditions, then $\preccurlyeq$ is a partial order relation (called lexicographic order for $\mathbf{S}$ ).

## Lexicographic order: example

- Let $\mathrm{A}=\{\mathrm{x}, \mathrm{y}\}$. Let R be the partial order relation on A :

$$
\mathrm{R}=\{(\mathrm{x}, \mathrm{x}),(\mathrm{x}, \mathrm{y}),(\mathrm{y}, \mathrm{y})\} .
$$

Let $S$ be the set of all strings over $A$, and $\preccurlyeq$ the lexicographic order for $S$ that corresponds to $R$.

## Examples:

$$
\begin{array}{ll}
\mathrm{x} \preccurlyeq \mathrm{xx} & \mathrm{x} \preccurlyeq \mathrm{xy} \\
\mathrm{yxy} \text { § } \mathrm{yxyxxx} & \mathrm{x} \preccurlyeq \mathrm{y} \\
\mathrm{xx} \preccurlyeq \mathrm{xyx} & \mathrm{xxxy} \mathrm{xy} \\
\varepsilon \preccurlyeq \mathrm{x} & \varepsilon \preccurlyeq \mathrm{xyxyy}
\end{array}
$$

## Hasse diagrams

- A Hasse diagram is a graph to present a partial order relation
- Example: Let A $=\{1,2,3,9,18\}$. Consider relation |on A: For all $\mathrm{a}, \mathrm{b} \in \mathrm{A}, \mathrm{a} \mid \mathrm{b} \Leftrightarrow \mathrm{b}=\mathrm{k} \cdot \mathrm{a}$ for some integer k .

Draw a directed graph of the relation, such that all arrows except loops point up.


Remove

1. loops at all vertices
2. arrows that are implied by the transitive property
3. direction indicators on the arrows


## Hasse diagrams: example

- The "subset" relation $\subseteq$ on $\operatorname{set} \mathrm{P}(\{a, b, c\})$ : for all $U$ and $V$ in $P(\{a, b, c\}), U \subseteq V \Leftrightarrow \forall x$, if $x \in U$ then $x \in V$ Draw directed graph of $\subseteq$ such that all arrows except loops point up. Remove all loops, unnecessary arrows, and direction indicators.



## Hasse diagrams: back to directed graph

- Obtain original directed graph from Hasse diagram:

1. Insert direction markers on the edges, making all arrows point up.
2. For each pair of arrows from one point to a second and from that second point to a third, add an arrow from the first point to the third; do so repeatedly until no more can be added.
3. Add loops at each vertex.


## Partially and totally ordered sets

- Let $\preccurlyeq$ be a partial order relation on a set A. Elements a and b of A are comparable if, and only, either $\mathrm{a} \preccurlyeq \mathrm{b}$ or $\mathrm{b} \preccurlyeq \mathrm{a}$.
Otherwise, $a$ and $b$ are noncomparable.
- Let R is a partial order relation on a set A . If every two elements in A are comparable, then R is a total order relation on A .
- Hasse diagram for a total order relation is a single vertical "chain".
- Set A is called a partially ordered set (or poset) with respect to a relation $\preccurlyeq$ if, and only if, $\preccurlyeq$ is a partial order relation on $A$.
- Set A is called a totally ordered set with respect to a relation $\preccurlyeq$ if, and only, A is a poset with respect to $\preccurlyeq$ and $\preccurlyeq$ is a total order.


## Partially and totally ordered sets (II)

- Let A be a poset with respect to a relation $\preccurlyeq$. Subset B of A is called a chain if, and only if, each pair of elements in B is comparable.
- The length of a chain is one less than the number of elements in the chain.
- Example:

Chain of subsets
The set $\mathrm{P}(\{\mathrm{a}, \mathrm{b}, \mathrm{c}\})$ is partially ordered with respect to $\subseteq$.
A chain of length 3: $\emptyset \subseteq\{a\} \subseteq\{a, b,\} \subseteq\{a, b, c\}$

## Partially and totally ordered sets (III)

- An element a in A is called a maximal element of A if, and only if, for all b in A , either $\mathrm{b} \preccurlyeq \mathrm{a}$ or b and a are not comparable.
- An element a in A is called a greatest element of A if, and only if, for all b in $\mathrm{A}, \mathrm{b} \preccurlyeq \mathrm{a}$. maximum
- An element a in A is called a minimal element of A if, and only if, for all $b$ in $A$, either $a \preccurlyeq b$ or $b$ and a are not comparable.
- An element a in A is called a least element of A if, and only if for all b in $\mathrm{A}, \mathrm{a} \preccurlyeq \mathrm{b}$.
minimum
- Example:
- a maximal element $g$
- greatest element: also $g$
- minimal elements: c, d, i
- there is no least element



## Topological sorting (partial to total order)

- Given partial order relations $\preccurlyeq$ and $\preccurlyeq$ ' on a set A, $\preccurlyeq '$ is compatible with $\preccurlyeq$ if, and only if,


## for all a and b in A , if $\mathrm{a} \preccurlyeq \mathrm{b}$ then $\mathrm{a} \preccurlyeq{ }^{\prime} \mathrm{b}$.

- Given partial order relations $\preccurlyeq$ and $\preccurlyeq$ ' on a set A, $\preccurlyeq \prime$ is a topological sorting for $\preccurlyeq i f$, and only if, $\preccurlyeq '$ is a total order that is compatible with $\preccurlyeq$.
- Example: $\mathrm{P}(\{\mathrm{a}, \mathrm{b}, \mathrm{c}\})$ with partial order $\subseteq$

Total order: $\emptyset,\{\mathrm{a}\},\{\mathrm{b}\},\{\mathrm{c}\},\{\mathrm{a}, \mathrm{b}\},\{\mathrm{a}, \mathrm{c}\},\{\mathrm{b}, \mathrm{c}\},\{\mathrm{a}, \mathrm{b}, \mathrm{c}\}$

## Topological sorting: algorithm

- Constructing a topological sorting

1. Pick any minimal element x in A with respect to $\preccurlyeq$.
[Such an element exists since A is nonempty.]
2. $\quad$ Set $A^{\prime}=A-\{x\}$
3. Repeat steps a to c while $A^{\prime} \neq \emptyset$ :
a. Pick any minimal element $y$ in A'.
b. Define $\mathrm{x} \preccurlyeq^{\prime} \mathrm{y}$.
c. $\quad \operatorname{Set} A^{\prime}=A^{\prime}-\{y\}$ and $x=y$.
