

Relations

- Given sets S and T , a **binary relation** from S to T is any subset R of $S \times T$ (i.e., $R \subseteq S \times T$).

- Example;

A university would be interested in the relation R consisting of all ordered pairs whose first entries are students and whose second entries are the courses the students are enrolled in. This relation is from the set S of university students to the set C of courses offered.

- If $s \in S$ is fixed:

$\{c \in C : (s,c) \in R\}$ - set of courses taken by s .

- If $c \in C$ is fixed:

$\{s \in S : (s,c) \in R\}$ - the class list for c .

- In case $S=T$, we say that a subset R of $S \times S$ is a **relation on S** .

- **Functions:**

A function $f: S \rightarrow T$, is a relation R_f from S to T such that for each $x \in S$ there is exactly one $y \in T$ with $(x,y) \in R_f$.

$$R_f = \{(x,y) \in S \times T : y = f(x)\}$$

- **R^- - Converse Relation:**

Given $R \subseteq S \times T$, the converse relation is defined as:

$$R^- = \{(y,x) \in T \times S : (x,y) \in R\}$$

Note: the converse function $f^- = \{(y,x) \in T \times S : y = f(x)\}$

Properties of Relations:

- A relation R on a set S is said to have the following properties if it satisfies the given condition for each property:

- **Reflexive - (R):**

$$(x,x) \in R \text{ for all } x \in S.$$

- **Antireflexive - (AR):**

$$(x,x) \notin R \text{ for all } x \in S.$$

- **Symmetric - (S):**

$$(x,y) \in R \text{ implies } (y,x) \in R \text{ for all } x,y \in S.$$

- **Antisymmetric - (AS):**

$$(x,y) \in R \text{ and } (y,x) \in R \text{ imply } x = y.$$

- **Transitive - (T):**

$$(x,y) \in R \text{ and } (y,z) \in R \text{ imply } (x,z) \in R.$$

- Examples:

- The Inequality Relation ' \leq ' on \mathbb{R} :

$$R = \{(x,y) \in \mathbb{R} \times \mathbb{R} : x \leq y\}$$

(R) $x \leq x$ for all $x \in \mathbb{R}$

(AS) $x \leq y$ and $y \leq x$ imply $x = y$

(T) $x \leq y$ and $y \leq z$ imply $x \leq z$

- The Strict Inequality Relation '<' on \mathbb{R} :

$$R = \{(x,y) \in \mathbb{R} \times \mathbb{R} : x < y\}$$

(AR) $x < x$ never holds

(T) $x < y$ and $y < z$ imply $x < z$

(AS) vacuously true

- Equality Relation '=' on S :

$$E = \{(x,y) \in S \times S : x = y\} = \{(x,x) : x \in S\}$$

(R); (S); (AS); (T)

- Example: Image of a subset under a relation

S = a set of suppliers.

T = a set of products.

$(x,y) \in R$ if supplier x sells product y .

Let $A \subseteq S$ and $B \subseteq T$,

$$R(A) = \{y \in T : (x,y) \in R \text{ for some } x \in A\}$$

(set of products sold by A)

$$R^-(B) = \{x \in S : (y,x) \in R \text{ for some } y \in B\}$$

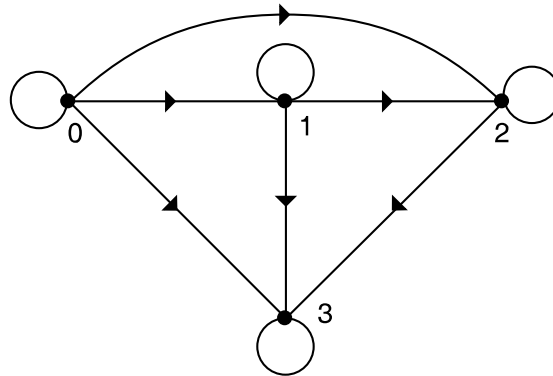
$$= \{x \in S : (x,y) \in R \text{ for some } y \in B\}$$

(set of suppliers for B)

Diagrams of Relations

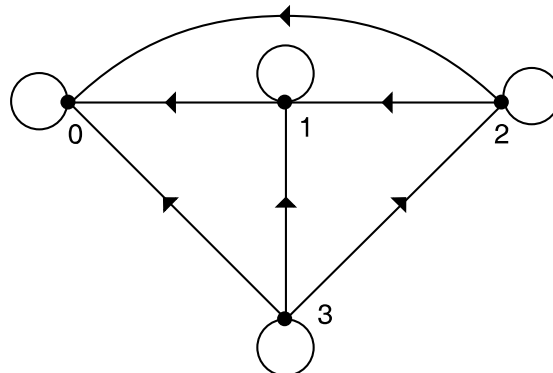
- Consider R_1 on $\{0,1,2,3\}$ defined by ' \leq ':

$$R_1 = \{(0,0), (0,1), (0,2), (0,3), (1,1), (1,2), (1,3), (2,2), (2,3), (3,3)\}$$



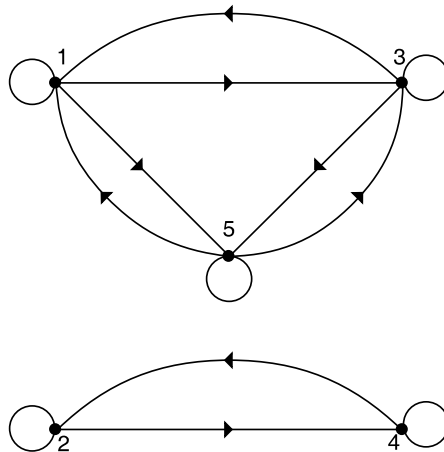
- Note: an arrow is drawn from m to n whenever $(m,n) \in R_1$. The arrows have been left off the loops.
- The diagram of the converse R_1^{-} relation is obtained by reversing the arrows in the figure. The loops remain unchanged.

$$R_1^{-} = \{(0,0), (1,0), (2,0), (3,0), (1,1), (2,1), (3,1), (2,2), (3,2), (3,3)\}$$

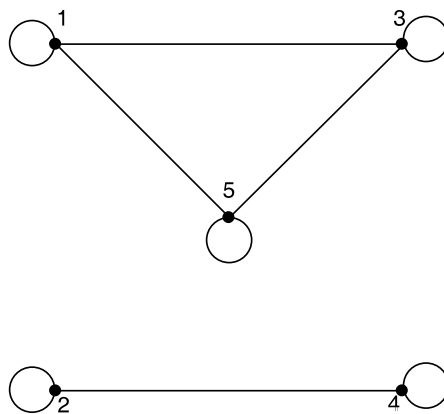


- Consider R_2 on $\{1,2,3,4,5\}$ defined by $(m,n) \in R_2$ iff $m-n$ is even:

$$R_2 = \{(1,1), (1,3), (1,5), (2,2), (2,4), (3,1), (3,3), (3,5), (4,2), (4,4), (5,1), (5,3), (5,5)\}$$



- Note: R_2 is symmetric.
- The diagram of R_2^{-1} is obtained by reversing the arrows in the diagram, but note you get the same picture. Hence $R_2^{-1} = R_2$
- When a relation is symmetric it is redundant to draw the arrows. The following diagram of R_2 is equally informative.



Digraphs

- **Directed Graphs (Digraphs):**

A **digraph** G consists of two sets,

$V(G)$ - the nonempty **set of vertices** of G ,

$E(G)$ - the **set of edges** of G ,

with a function $\gamma: E(G) \rightarrow V(G) \times V(G)$.

- if $\gamma(e) = (p,q)$, then e **goes from p to q** and:

p - the **initial (source) vertex** of e ,

q - the **terminal (final) vertex** of e .

- **Picture of a Digraph:**

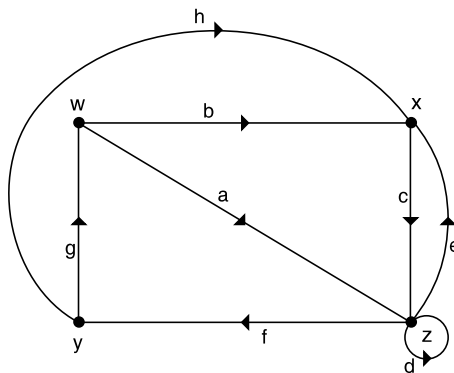
A **picture** of a digraph G is a diagram consisting of points, corresponding to the members of $V(G)$, and directed arcs corresponding to the members of $E(G)$, so that if $\gamma(e) = (p,q)$, then a directed arc corresponding to e is drawn from the point labeled p to the point labeled q .

- **Example:**

$V(G) = \{w,x,y,z\}$; $E(G) = \{a,b,c,d,e,f,g,h\}$

$\gamma(a) = (w,z)$; $\gamma(b) = (w,x)$; $\gamma(c) = (x,z)$; $\gamma(d) = (z,z)$;

$\gamma(e) = (z,x)$; $\gamma(f) = (z,y)$; $\gamma(g) = (y,w)$; $\gamma(h) = (y,x)$;



Paths in Digraphs

- A **path** in a digraph G is a **sequence of edges** such that the terminal vertex of one edge is the initial vertex of the next.

For $e_1, \dots, e_n \in E(G)$, e_1, e_2, \dots, e_n is a path provided there are vertices $x_1, x_2, \dots, x_n, x_{n+1}$ so that $\gamma(e_i) = (x_i, x_{i+1})$ for $i=1, 2, \dots, n$.

- **Path Length:**

The **length** of a path is the number of edges in the path.

- **Closed Path:**

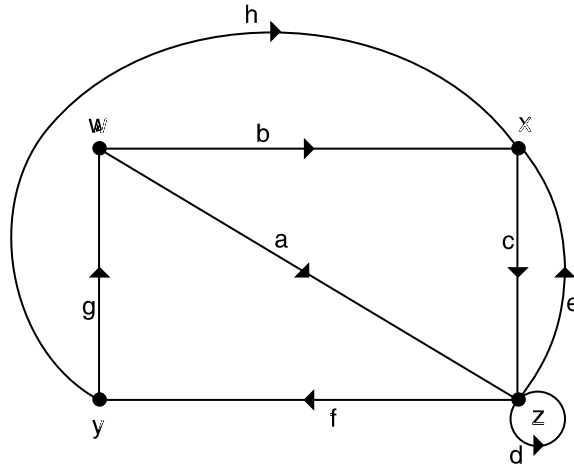
A path is **closed** if $x_1 = x_{n+1}$.

- **Cycle:**

A closed path, $x_1, x_2, \dots, x_n, x_1$, of length at least 1, is called a **cycle** if x_1, x_2, \dots, x_n are all different.

- **Acyclic Digraph (DAG):**

A digraph with no cycles is called acyclic.



● Examples:

f g a e - path of length 4 from z to x.

c e c e c and f g a f h c - paths

f a - not a path

f g a f h c and c e c e - closed paths

f h c e and d f - paths but not closed

a f g and c f h - cycles

c e - cycle

d - cycle

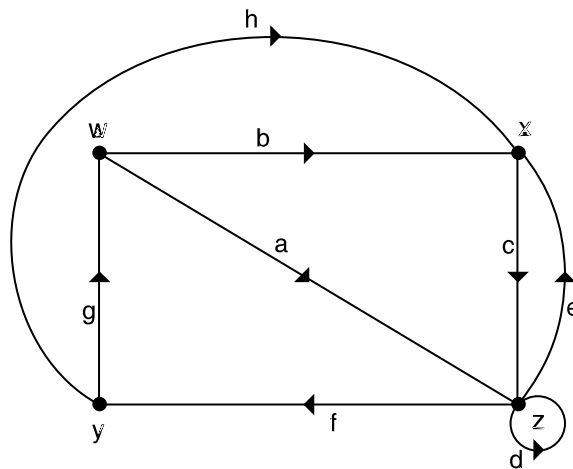
c f g a e - closed path but not a cycle

Adjacency Relation

- Given a digraph G and vertices v and w in $V(G)$, v is **adjacent** to w if there is an edge in $E(G)$ from v to w .
- **Adjacency Relation 'A' on $V(G)$:**

$$A = \{(v,w) \in V(G) \times V(G) : v \text{ is adjacent to } w\} = \gamma(E(G))$$

- **Example:**



$$A = \{(w,z), (w,x), (x,z), (z,z), (z,x), (z,y), (y,w), (y,x)\}$$

Graphs

- **Graphs:**

A **graph** G consists of two sets,

$V(G)$ - the nonempty **set of vertices** of G ,

$E(G)$ - the **set of edges** of G ,

with a function $\gamma: E(G) \rightarrow \{\{u,v\} : u,v \in V(G)\}$

- For an edge e in $E(G)$, the members of $\gamma(e)$ are called the **vertices** or **endpoints** of e . We say e **joins** its endpoints.

- A **loop** is an edge with only one endpoint.

- Distinct edges e and f with $\gamma(e) = \gamma(f)$ are called **parallel** or **multiple** edges.

- **Picture of a Graph:**

A **picture** of a graph G is a diagram consisting of points, corresponding to the members of $V(G)$, and undirected arcs corresponding to the members of $E(G)$, so that if $\gamma(e) = \{u,v\}$, then an arc corresponding to e is drawn from the point labeled u to the point labeled v .

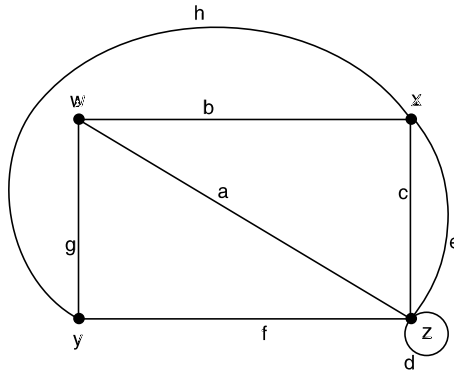
- A **path of length n** from vertex u to vertex v in a graph G is a **sequence of edges** e_1, e_2, \dots, e_n **together with a sequence of vertices** $x_1, x_2, \dots, x_n, x_{n+1}$ with $\gamma(e_i) = \{x_i, x_{i+1}\}$ for $i=1, 2, \dots, n$ and $x_1 = u, x_{n+1} = v$. If $u = v$, the path is **closed**.

● Example:

$$V(G) = \{w,x,y,z\}; E(G) = \{a,b,c,d,e,f,g,h\}$$

$$\gamma(a)=\{w,z\}; \gamma(b)=\{w,x\}; \gamma(c)=\{x,z\}; \gamma(d)=\{z,z\} \text{ or } \{z\};$$

$$\gamma(e)=\{z,x\}; \gamma(f)=\{z,y\}; \gamma(g)=\{y,w\}; \gamma(h)=\{y,x\};$$



The Path

Its Vertex Sequence

f g b

z y w x

e a b c

x z w x z

c a b e

x z w x z

f d a

y z z w - uses the loop

f d a a d d a

y z z w z z z w - reuse of edges

f c b g

y z x w y - closed

c e

x z x

c e

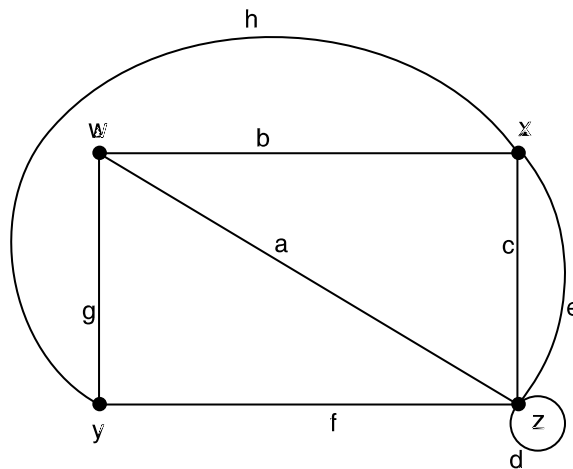
z x z

Adjacency Relation

- Given a graph (or digraph) G and vertices v and w in $V(G)$, v is **adjacent** to w if there is an edge in $E(G)$ from v to w .
- **Adjacency Relation 'A' on $V(G)$:**

$$A = \{(v,w) \in V(G) \times V(G) : v \text{ is adjacent to } w\}$$

- **Example:**



$$A = \{(w,x), (w,y), (w,z), (x,w), (x,y), (x,z), (y,w), (y,x), (y,z), (z,w), (z,x), (z,y), (z,z)\}$$

- **Reachable Relation 'R' on $V(G)$:**
 $R = \{(v,w) \in V(G) \times V(G) : \text{there is a path of length at least 1 in } G \text{ from } v \text{ to } w\}$
- In the above figure all vertices are reachable from all other vertices; therefore, $R = \{\text{all possible ordered pair}\}$

Matrices

- A **matrix** is a rectangular array of elements.
- If a_{ij} is the entry in the i th row and j th column of matrix **A**, we can then write:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} = [a_{ij}]$$

- The above matrix **A** is an **$m \times n$ matrix** (m rows and n columns).
- $a_{ij} = \mathbf{A}[i,j]$.
- Example - 3×5 matrix:

$$\mathbf{A} = \begin{bmatrix} 2 & -1 & 0 & 3 & 2 \\ 1 & -2 & 1 & -1 & 3 \\ 3 & 0 & 1 & 2 & -3 \end{bmatrix}$$

- $\mathcal{M}_{m,n}$ is defined as the set of all $m \times n$ matrices.

- **Equality of Matrices:**

Two matrices \mathbf{A} and \mathbf{B} in $\mathcal{M}_{m,n}$ are **equal** provided that all their corresponding entries are equal; i.e.,

$$\mathbf{A} = \mathbf{B} \text{ provided } a_{ij} = b_{ij} \text{ for all } i,j.$$

- **Transpose of a Matrix:**

The transpose \mathbf{A}^T of a matrix \mathbf{A} in $\mathcal{M}_{m,n}$ is the matrix in $\mathcal{M}_{n,m}$ such that

$$\mathbf{A}^T[i,j] = \mathbf{A}[j,i]$$

$$\mathbf{A} = \begin{bmatrix} 2 & -1 & 0 & 3 & 2 \\ 1 & -2 & 1 & -1 & 3 \\ 3 & 0 & 1 & 2 & -3 \end{bmatrix} \quad \mathbf{A}^T = \begin{bmatrix} 2 & 1 & 3 \\ -1 & -2 & 0 \\ 0 & 1 & 1 \\ 3 & -1 & 2 \\ 2 & 3 & -3 \end{bmatrix}$$

- A matrix \mathbf{A} is **symmetric** if $\mathbf{A} = \mathbf{A}^T$.
- $1 \times n$ matrices are call **row vectors**.
- $m \times 1$ matrices are called **column vectors**.

$$\mathbf{v}_1 = [2 \quad -1 \quad 3] \quad \mathbf{v}_2 = \begin{bmatrix} 2 \\ -1 \\ 3 \end{bmatrix}$$

- **Matrix Sum:**

If $\mathbf{A} = [a_{ij}]$, $\mathbf{B} = [b_{ij}] \in \mathcal{M}_{m,n}$, then $\mathbf{A} + \mathbf{B} = \mathbf{C} = [c_{ij}] \in \mathcal{M}_{m,n}$ with $c_{ij} = a_{ij} + b_{ij}$ for all i, j .

or

$$(\mathbf{A} + \mathbf{B})[i,j] = \mathbf{A}[i,j] + \mathbf{B}[i,j] \text{ for all } i, j.$$

- **Example:**

$$\mathbf{A} = \begin{bmatrix} 2 & 4 & 0 \\ -1 & 3 & 2 \\ -3 & 1 & 2 \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} 1 & 0 & 5 & 3 \\ 2 & 3 & -2 & 1 \\ \blacktriangleleft & -2 & 0 & 2 \end{bmatrix} \quad \mathbf{C} = \begin{bmatrix} 3 & 1 & -2 \\ -5 & 0 & 2 \\ -2 & \blacktriangleleft & 1 \end{bmatrix}$$

$$\mathbf{A} + \mathbf{C} = \begin{bmatrix} 5 & 5 & -2 \\ -6 & 3 & \blacktriangleleft \\ -5 & 5 & 3 \end{bmatrix}$$

$$\mathbf{B} + \mathbf{B} = \begin{bmatrix} 2 & 0 & 10 & 6 \\ \blacktriangleleft & 6 & -\blacktriangleleft & 2 \\ 8 & -\blacktriangleleft & 0 & \blacktriangleleft \end{bmatrix}$$

- **Notes:**

$\mathbf{A} + \mathbf{B}$ and $\mathbf{B} + \mathbf{C}$ are not defined.

$\mathbf{A} + \mathbf{A}$ and $\mathbf{C} + \mathbf{C}$ can be calculated if desired.

- Notes:

$\mathbf{0}$ represents the $m \times n$ matrix with all entries of 0.

If $\mathbf{A} = [a_{ij}]$, then $-\mathbf{A} = [-a_{ij}]$ ($-\mathbf{A}$ is the negative of \mathbf{A}).

- **Theorem:**

For \mathbf{A}, \mathbf{B} , and \mathbf{C} in $\mathcal{M}_{m,n}$

- a) $\mathbf{A} + (\mathbf{B} + \mathbf{C}) = (\mathbf{A} + \mathbf{B}) + \mathbf{C}$ (associative law)
- b) $\mathbf{A} + \mathbf{B} = \mathbf{B} + \mathbf{A}$ (commutative law)
- c) $\mathbf{A} + \mathbf{0} = \mathbf{0} + \mathbf{A} = \mathbf{A}$ (additive identity)
- d) $\mathbf{A} + (-\mathbf{A}) = (-\mathbf{A}) + \mathbf{A} = \mathbf{0}$ (additive inverses)

- **Scalar Multiplication:**

Given $\mathbf{A} \in \mathcal{M}_{m,n}$ and $c \in \mathbb{R}$, $c\mathbf{A} \in \mathcal{M}_{m,n}$ with (i,j) entry of ca_{ij} ,

$$\text{or } (c\mathbf{A})[i,j] = c\mathbf{A}[i,j]$$

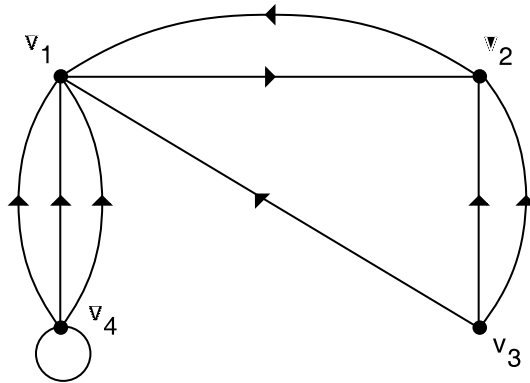
$c\mathbf{A}$ is called the **scalar product** of c and \mathbf{A} .

- Example:

$$\mathbf{A} = \begin{bmatrix} 2 & 1 & -3 \\ -1 & 0 & 4 \end{bmatrix} \quad 2\mathbf{A} = \begin{bmatrix} 4 & 2 & -6 \\ -2 & 0 & 8 \end{bmatrix} \quad -7\mathbf{A} = \begin{bmatrix} -14 & -7 & 21 \\ 7 & 0 & -28 \end{bmatrix}$$

The Adjacency Matrix

- Consider a finite graph (or digraph) G with vertex set $V(G)$.
- Let v_1, v_2, \dots, v_n be a list of the vertices in $V(G)$.
- The **adjacency matrix**, is a square $n \times n$ matrix \mathbf{M} such that m_{ij} = the number of edges from v_i to v_j .

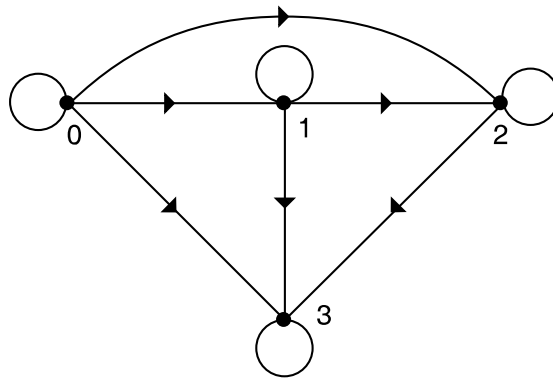


$$\mathbf{M} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 3 & 0 & 0 & 1 \end{bmatrix}$$

The Adjacency Matrix and Relations

- Every relation R on a finite set S corresponds to a finite digraph G with no multiple edges.
- Hence, it also corresponds to a matrix M_R of 0's and 1's
- Consider R_1 on $S = \{0,1,2,3\}$ defined by ' \leq ':

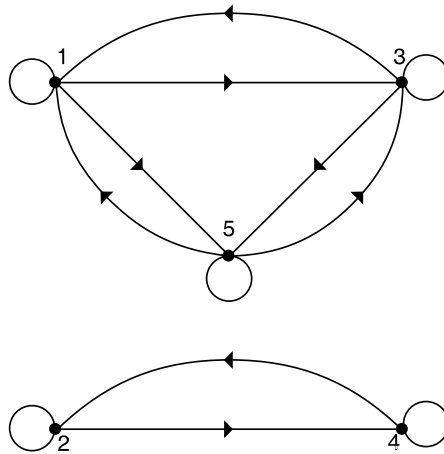
$$R_1 = \{(0,0),(0,1),(0,2),(0,3),(1,1),(1,2),(1,3),(2,2),(2,3),(3,3)\}$$



$$M_{R_1} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- Consider R_2 on $S = \{1,2,3,4,5\}$ defined by $(m,n) \in R_2$ iff $m - n$ is even:

$$R_2 = \{(1,1), (1,3), (1,5), (2,2), (2,4), (3,1), (3,3), (3,5), (4,2), (4,4), (5,1), (5,3), (5,5)\}$$



$$M_{R_2} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

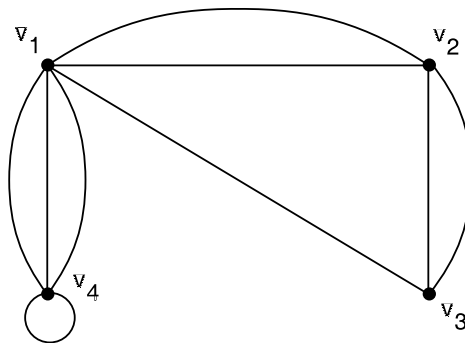
- The matrix of the converse R^{-} of a relation R is the transpose of the matrix for R .

$$\mathbf{M}_{R^{-}} = \mathbf{M}_R^T$$

- Consider R_1 on $S = \{0,1,2,3\}$ defined by ' \leq ':

$$\mathbf{M}_{R_1^{-}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

- A relation R is **symmetric** iff $\mathbf{M}_R = \mathbf{M}_R^T$.



$$\mathbf{M} = \begin{bmatrix} 0 & 2 & 1 & 3 \\ 2 & 0 & 2 & 0 \\ 1 & 2 & 0 & 0 \\ 3 & 0 & 0 & 1 \end{bmatrix}$$

Multiplication of Matrices

- Two matrices **A** and **B** can be multiplied to get a **product matrix C = AB**, provided that the number of columns of **A** equals the number of rows of **B**.

- If **A** is an $m \times n$ matrix and **B** is an $n \times p$ matrix, then **C = AB** is an $m \times p$ matrix defined by

$$c_{ik} = \sum_{j=1}^n a_{ij}b_{jk} \quad \text{for } 1 \leq i \leq m \quad \text{and} \quad 1 \leq k \leq p.$$

- Examples:

$$\mathbf{A} = \begin{bmatrix} 3 & -1 \\ -2 & \blacktriangleleft \end{bmatrix} \quad \mathbf{B} = \begin{bmatrix} -1 & 0 & 3 \\ 2 & 1 & -5 \end{bmatrix} \quad \mathbf{v}_1 = [2 \quad -3 \quad \blacktriangleleft] \quad \mathbf{v}_2 = \begin{bmatrix} 1 \\ -3 \end{bmatrix}$$

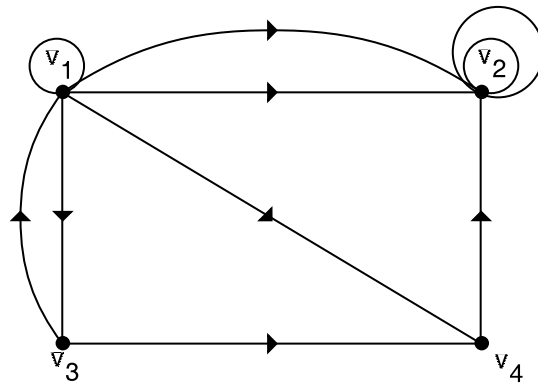
$$\mathbf{AB} = \begin{bmatrix} 3 & -1 \\ -2 & \blacktriangleleft \end{bmatrix} \begin{bmatrix} -1 & 0 & 3 \\ 2 & 1 & -5 \end{bmatrix} = \begin{bmatrix} -5 & -1 & 1\blacktriangleleft \\ 10 & \blacktriangleleft & -26 \end{bmatrix}$$

$$\mathbf{A}^2 = \mathbf{AA} = \begin{bmatrix} 3 & -1 \\ -2 & \blacktriangleleft \end{bmatrix} \begin{bmatrix} 3 & -1 \\ -2 & \blacktriangleleft \end{bmatrix} = \begin{bmatrix} 11 & -7 \\ -1\blacktriangleleft & 18 \end{bmatrix}$$

$$\mathbf{Av}_2 = \begin{bmatrix} 3 & -1 \\ -2 & \blacktriangleleft \end{bmatrix} \begin{bmatrix} 1 \\ -3 \end{bmatrix} = \begin{bmatrix} 6 \\ -1\blacktriangleleft \end{bmatrix}$$

$$\mathbf{v}_2\mathbf{v}_1 = \begin{bmatrix} 1 \\ -3 \end{bmatrix} [2 \quad -3 \quad \blacktriangleleft] = \begin{bmatrix} 2 & -3 & \blacktriangleleft \\ -6 & 9 & -12 \end{bmatrix}$$

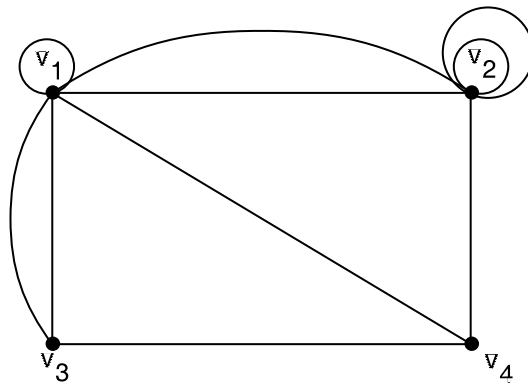
- The powers of adjacency matrices can be used to count the number of paths between vertex pairs in graphs (or digraphs).
- The (i,j) entry in \mathbf{M}^k gives the number of paths of length k from vertex i to vertex j .



$$\mathbf{M} = \begin{bmatrix} 1 & 2 & 1 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \quad \mathbf{M}^2 = \begin{bmatrix} 2 & 7 & 1 & 2 \\ 0 & 4 & 0 & 0 \\ 1 & 3 & 1 & 1 \\ 0 & 2 & 0 & 0 \end{bmatrix}$$

$$\mathbf{M}^3 = \mathbf{M}\mathbf{M}^2 = \begin{bmatrix} 1 & 2 & 1 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & 7 & 1 & 2 \\ 0 & 4 & 0 & 0 \\ 1 & 3 & 1 & 1 \\ 0 & 2 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 20 & 2 & 3 \\ 0 & 8 & 0 & 0 \\ 2 & 9 & 1 & 2 \\ 0 & 4 & 0 & 0 \end{bmatrix}$$

● Example:



$$\mathbf{M} = \begin{bmatrix} 1 & 2 & 2 & 1 \\ 2 & 2 & 0 & 1 \\ 2 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad \mathbf{M}^2 = \begin{bmatrix} 10 & 7 & 3 & 5 \\ 7 & 9 & 5 & 4 \\ 3 & 5 & 5 & 2 \\ 5 & 4 & 2 & 3 \end{bmatrix}$$

$$\mathbf{M}^3 = \mathbf{M}\mathbf{M}^2 = \begin{bmatrix} 1 & 2 & 2 & 1 \\ 2 & 2 & 0 & 1 \\ 2 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 10 & 7 & 3 & 5 \\ 7 & 9 & 5 & 4 \\ 3 & 5 & 5 & 2 \\ 5 & 4 & 2 & 3 \end{bmatrix} = \begin{bmatrix} 35 & 39 & 25 & 20 \\ 39 & 36 & 18 & 21 \\ 25 & 18 & 8 & 13 \\ 20 & 21 & 13 & 11 \end{bmatrix}$$

- **Associative Law for Matrices:**

If **A** is a $m \times n$ matrix, **B** is an $n \times p$ matrix, and **C** is a $p \times q$ matrix, then $(\mathbf{AB})\mathbf{C} = \mathbf{A}(\mathbf{BC})$.

- Note: Multiplication of matrices is **not commutative**.

- **The Identity Matrix - I:**

The identity matrix **I** is an $n \times n$ matrix where:

$$\begin{aligned} \mathbf{I}[i,i] &= 1 && \text{for } i = 1, 2, \dots, n \\ \mathbf{I}[i,j] &= 0 && \text{for } i \neq j. \end{aligned}$$

$$\mathbf{I} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{bmatrix}$$

- \mathbf{I}_n is an identity matrix of size n (i.e., an $n \times n$ matrix)

- $\mathbf{A}\mathbf{I}_n = \mathbf{I}_n\mathbf{A} = \mathbf{A}$

- $\mathbf{I}_n \mathbf{I}_n = \mathbf{I}_n$

- $(\mathbf{I}_n)^k = \mathbf{I}_n$

Equivalence Relations and Partitions

- A relation is an **equivalence relation** if it is **reflexive, symmetric, and transitive.**

- Example:

Let S be a set marbles. We define a relation \sim on S as "has the same color as". Relation \sim is an equivalence relation since, for marbles s , t , and u :

(R) $s \sim s$ for all marbles s ,

(S) If $s \sim t$, then $t \sim s$,

(T) If $s \sim t$ and $t \sim u$, then $s \sim u$.

Note: we can break up S into disjoint subsets so that elements belong to the same subset iff they are equivalent (i.e., iff they have the same color).

- **Partitions:**

A **partition** of a nonempty set S is a collection of nonempty subsets that are disjoint and whose union is S .

- Example:

Let C be the set of colors of the marbles and define the function $f: S \rightarrow C$ by $f(s) = \text{'the color of } s\text{'}$ for each s in S .

Then, the partition $\{f^{-1}(c) : c \in C\}$ is the set of subsets of S such that the member marbles of each subset have the same color.

● **Equivalence Classes:**

- Consider an equivalence relation \sim on a set S .
- For each $s \in S$ we define
$$[s] = \{t \in S : s \sim t\}$$
- The set $[s]$ is called the **equivalence class** containing s .
- The set of all equivalence classes of S is $[S]$ where
$$[S] = \{[s] : s \in S\}$$

● Example - the marble example:

- $[s]$ is the set of all marbles that are the same color as s .
- $[S] = \{\{\text{blue marbles}\}, \{\text{red marbles}\}, \{\text{green marbles}\}, \dots\}$

● Example:

Define \sim on $\mathbb{N} \times \mathbb{N}$ by $(m,n) \sim (j,k)$ provided that $m^2+n^2=j^2+k^2$.

i.e., The relation = $\{((m,n),(j,k)), \dots\}$

Test \sim to see if it is an equivalence relation:

(R) $(m,n) \sim (m,n)$ for all (m,n)

(S) If $(m,n) \sim (j,k)$, then $(j,k) \sim (m,n)$

(T) If $(m,n) \sim (j,k)$ and $(j,k) \sim (p,q)$, then $(m,n) \sim (p,q)$

Hence, \sim is an equivalence relation

$$[(0,10)] = \{(0,10),(6,8),(8,6),(10,0)\}$$

$$[(0,5)] = [(3,4)] = [(4,3)] = [(5,0)] = \{(0,5),(3,4),(4,3),(5,0)\}$$

$$[\mathbb{N} \times \mathbb{N}] = \{\{(0,0)\}, \{(0,1),(1,0)\}, \{(1,1)\}, \{(0,2),(2,0)\}, \dots\}$$

● **Lemma:**

Let \sim be an equivalence relation on a set S . For $s, t \in S$ the following assertions are logically equivalent (i.e., all are true or all are false):

- a) $s \sim t$
- b) $[s] = [t]$
- c) $[s] \cap [t] \neq \emptyset$

● **Theorem:**

- If \sim is an equivalence relation on a nonempty set S , then $[S]$ is a partition on S .
- Conversely, if $\{A_i : i \in I\}$ is a partition on S , then the sets A_i are the equivalence classes corresponding to some equivalence relation on S .

● **Theorem:**

- (a) Let S be a nonempty set. Let $f: S \rightarrow T$. Define $s_1 \sim s_2$ if $f(s_1) = f(s_2)$. Then \sim is an equivalence relation on S , and the equivalence classes are the nonempty sets $f^{-1}(t)$, $t \in T$.
- (b) Every equivalence relation \sim on a set S is determined by a suitable function with domain S , as in part (a).

● **Natural Mapping Function v :**

$v: S \rightarrow [S]$ is defined by $v(s) = [s]$

● Example:

S = the set of marbles,

T = the set of colors,

$f: S \rightarrow T$ such that $f(s)$ = the color of s ,

$v(s) = [s]$ = the set of all marbles the same color as s .

$[S] = \{ \text{the nonempty sets of } f^{-1}(t) : t \in T \}$

● Example:

Define \sim on $\mathbb{N} \times \mathbb{N}$ by $(m,n) \sim (j,k)$ provided that $m^2+n^2=j^2+k^2$.

Define $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ by the rule $f(m,n) = m^2 + n^2$.

$[\mathbb{N} \times \mathbb{N}] = \{ \text{the nonempty sets of } f^{-1}(r) : r \in \mathbb{N} \}$

● Example:

Define \sim on $\mathbb{R} \times \mathbb{R}$ by $(x,y) \sim (z,w)$ provided $x^2+y^2=z^2+w^2$.

Define $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ by the rule $f(x,y) = x^2 + y^2$.

The equivalence classes are the circles in the plane $\mathbb{R} \times \mathbb{R}$ centered at $(0,0)$.

The function v maps each point (x,y) to the circle on which it lies.

The Division Algorithm

- **The Division Algorithm (Integer Division):**

Let $p \in \mathbb{P}$. For each $n \in \mathbb{Z}$ there exists $q \in \mathbb{Z}$ and $r \in \mathbb{N}$ such that
 $n = p \cdot q + r$ and $0 \leq r < p$.

- When n is **divided by** p
 q is called the **quotient**,
 r is called the **remainder**.

- If we rewrite the conditions of the algorithm as:

$$\frac{n}{p} = q + \frac{r}{p} \quad \text{with} \quad 0 \leq \frac{r}{p} < 1 \quad \text{then}$$

$q =$ integer part of $n/p = \lfloor n/p \rfloor$

$r/p =$ fractional part of n/p

where $\lfloor x \rfloor =$ greatest integer less than or equal to x
(another name for $\lfloor \ \rfloor$ is the **floor function**)

$$r = (n/p - \lfloor n/p \rfloor) \cdot p \quad \text{or} \quad (r = n - q \cdot p)$$

- Example: $n = 31$; $p = 7$

$$n/p \approx 4.429$$

$$q = \lfloor 31/7 \rfloor = 4; \quad r = (31/7 - 4)7 = 3$$

$$r = (31 - 28) = 3$$

- Example: $n = -31$; $p = 7$

$$n/p \approx -4.429$$

$$q = \lfloor -31/7 \rfloor = -5; \quad r = (-31/7 - (-5))7 = 4$$

$$r = (-31 - (-7)(-5)) = +4$$

$\mathbb{Z}(p)$

- Given $p \in \mathbb{P}$, $n \text{ MOD } p = (n/p - \lfloor n/p \rfloor) \cdot p = \text{the remainder mod } p$.
- $\mathbb{Z}(p) = \{0, 1, 2, \dots, p-1\}$
- $\text{MOD } p$ is a function such that $\text{MOD } p: \mathbb{Z} \rightarrow \mathbb{Z}(p)$
- $\text{MOD } p$ maps \mathbb{Z} onto $\mathbb{Z}(p)$ since $n \text{ MOD } p = n$ for $n \in \mathbb{Z}(p)$.
- **Congruence mod p - the relation ' $\equiv \pmod{p}$ ':**
For $m, n \in \mathbb{Z}$, we define
 $m \equiv n \pmod{p}$ in case $m \text{ MOD } p = n \text{ MOD } p$.
- Congruence mod p is an equivalence relation on \mathbb{Z} determined by the function $\text{MOD } p: \mathbb{Z} \rightarrow \mathbb{Z}(p)$.
- **Theorem:**
Let $p \in \mathbb{P}$. For $m, n \in \mathbb{Z}$, we have
 $m \equiv n \pmod{p}$ iff $m - n$ is multiple of p .
- **Congruence Class mod p - $[n]_p$:**
The equivalence class of n with respect to the equivalence relation $\equiv \pmod{p}$ is called its congruence class mod p .
 $[n]_p = \{m \in \mathbb{Z}: m \equiv n \pmod{p}\}$.
- **Example:**
 $[0]_2 = [2]_2 = [4]_2 = \{n \in \mathbb{Z} : n \text{ is even}\}$
 $[1]_2 = [-3]_2 = [7]_2 = \{n \in \mathbb{Z} : n \text{ is odd}\}$

● **Theorem:**

Let $m, m', n, n' \in \mathbb{Z}$ and let $p \in \mathbb{P}$.

If $m' \equiv m \pmod{p}$ and $n' \equiv n \pmod{p}$, then

- (a) $m' + n' \equiv m + n \pmod{p}$,
- (b) $m' \cdot n' \equiv m \cdot n \pmod{p}$.

● **Corollary:**

Let $m, n \in \mathbb{Z}$ and $p \in \mathbb{P}$. Then

- (a) $(m \text{ MOD } p + n \text{ MOD } p) \equiv m + n \pmod{p}$,
- (b) $(m \text{ MOD } p) \cdot (n \text{ MOD } p) \equiv m \cdot n \pmod{p}$.

● The operators $+_p$ and $*_p$ on $\mathbb{Z}(p)$:

For $j, k \in \mathbb{Z}(p)$:

$$j +_p k = (j + k) \text{ MOD } p$$

$$j *_p k = (jk) \text{ MOD } p$$

● **Theorem:**

Let $m, n \in \mathbb{Z}$ and $p \in \mathbb{P}$. Then

- (a) $(m + n) \text{ MOD } p = (m \text{ MOD } p) +_p (n \text{ MOD } p)$
- (b) $(m \cdot n) \text{ MOD } p = (m \text{ MOD } p) *_p (n \text{ MOD } p)$

● **Example:**

$$(6 + 3) \text{ MOD } 2 = 9 \text{ MOD } 2 = 1$$

$$(6 + 3) \text{ MOD } 2 = 6 \text{ MOD } 2 +_2 3 \text{ MOD } 2 = 0 +_2 1 = 1$$

$$(8 \cdot 3) \text{ MOD } 6 = 24 \text{ MOD } 6 = 0$$

$$(8 \cdot 3) \text{ MOD } 6 = 8 \text{ MOD } 6 *_6 3 \text{ MOD } 6 = 2 *_6 3 = 0$$

● **Theorem:**

Let $m, n, r \in \mathbb{Z}$ and $p \in \mathbb{P}$. Then

- (a) $m +_p n = n +_p m$ and $m *_p n = n *_p m$
- (b) $(m +_p n) +_p r = m +_p (n +_p r)$ and
 $(m *_p n) *_p r = m *_p (n *_p r)$
- (c) $(m +_p n) *_p r = (m *_p r) +_p (n *_p r)$