

Functions must be well defined

Recall that a function $f: A \rightarrow B$ is a rule assigning every element a of A to a unique (ie, exactly one) element b of B . (Or more formally a function from A to B is a relation f from A to B (i.e., $f \subseteq A \times B$) such that for every $a \in A$ there is a unique $b \in B$ such that $(a, b) \in f$.) The underlined part can be rewritten as " $(\forall a \in A)(\exists! b \in B)(f(a) = b)$ ". Consider its negation. "For some $a \in A$, either there is no b such that $f(a) = b$ or there is more than one b such that $f(a) = b$ "

$$\underbrace{a_1 = a_2 \text{ but } f(a_1) \neq f(a_2)}_{\equiv \neg (a_1 = a_2 \Rightarrow f(a_1) = f(a_2))} \quad (\text{by putting } a = a_1 = a_2, b_i = f(a_i))$$

Thus the underlined part can be written as " $(\forall a \in A)(\exists b \in B)(f(a) = b)$ and $(\forall a_1, a_2 \in A)(a_1 = a_2 \Rightarrow f(a_1) = f(a_2))$ "

This property of a function is referred by saying that " f is well defined"

Definition: Let $f: A \rightarrow B$ be a rule assigning every element of A to an element of B (or equivalently, f is a relation from A to B with domain A). We say that f is well defined if

For all $a_1, a_2 \in A$, $a_1 = a_2$ implies $f(a_1) = f(a_2)$.

Remark: Functions must be well defined. Whenever the domain of a function f consists of elements with more than one representatives (such as the domain is a quotient set so that its elements are equivalence classes) and the rule of f depends on the representatives, we need to justify that f is well defined.

Ex: Consider the functions $f: \mathbb{Z} \rightarrow \{-1, 1\}$ and $g: \mathbb{Z}_3 \rightarrow \{-1, 1\}$
 $n \mapsto (-1)^n$ and $[n]_3 \mapsto (-1)^n$

Consider first f . The elements of its domain \mathbb{Z} has no different representatives. That is, two elements n_1 and n_2 of \mathbb{Z} are the same if and only if they have the same representatives n_1 and n_2 . So for f we don't really need to check that f is well defined because it is trivially true. That is, " $n_1 = n_2 \Rightarrow (-1)^{n_1} = (-1)^{n_2}$ " is true for obvious reasons.

Consider now g . The elements of its domain \mathbb{Z}_2 have many different representatives. As the rule of g depends on the representatives, we need to justify that g is well defined (i.e., the rule of g gives the same element of $\{-1, 1\}$ when the different representatives of an element are used). For instance, $[1]_3$ and $[4]_3$ are representatives of the same element of \mathbb{Z}_3 , so their images under g must be the same. But $g([1]_3) = (-1)^1 = -1$ and $g([4]_3) = (-1)^4 = 1$ are not the same. So g is not well defined (because $[1]_3 = [4]_3$ but $g([1]_3) \neq g([4]_3)$). Hence, g is not a function.

Ex: Let m and n be positive integers. Show that there is a well defined function $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ given by $f([a]_m) = [a]_n$ if and only if $m|n$.

Sol: (\Rightarrow) Suppose that f is well defined. As $[0]_m = [m]_m$, it follows that $f([0]_m) = f([m]_m)$ and so $[0]_n = [m]_n$. This shows that $0 \equiv m \pmod{n}$, and so $n|0-m$, implying that $n|m$.

(\Leftarrow) Suppose that $n|m$. Let $[a_1]_m = [a_2]_m$ where $[a_i]_m \in \mathbb{Z}_m$. Then $m|a_1 - a_2$. As $n|m$, it follows that $n|a_1 - a_2$, implying that $[a_1]_n = [a_2]_n$. So $f([a_1]_m) = f([a_2]_m)$. Hence f is well defined.

(Binary) Operations on a set

By a binary operation on a set A we mean any function $f: A \times A \rightarrow A$ (from $A \times A$ to A). So it takes two elements a_1, a_2 of A and gives an element $f(a_1, a_2)$ of A . We usually abuse the notation to write $a_1 f a_2$ instead of $f(a_1, a_2)$, which is useful when we consider arithmetic

operations. For instance the usual addition $+$ is a binary operation on \mathbb{R} , it is indeed a function $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$. For instance $+(2, 3) = 2 + 3 = 5$.

Remark: A binary operation $*$ on a set A (i.e., a function $*$: $A \times A \rightarrow A$) must be well defined. That is, " $(\forall a_1, b_1, a_2, b_2 \in A) (a_1 = a_2 \text{ and } b_1 = b_2 \Rightarrow a_1 * b_1 = a_2 * b_2)$ "

Remark: (Modular Arithmetic)

Let n be a positive integer. Consider $\mathbb{Z}_n = \{[k]_n \mid k \in \mathbb{Z}\}$, the integers modulo n . Recall for any $k_1, k_2 \in \mathbb{Z}$ that " $[k_1]_n = [k_2]_n \Leftrightarrow k_1 \equiv k_2 \pmod{n} \Leftrightarrow n \mid k_1 - k_2$ " and for any $k \in \mathbb{Z}$ that $[k]_n = \{t \in \mathbb{Z} \mid k \equiv t \pmod{n}\}$. We may do arithmetic in \mathbb{Z}_n , that is we may define addition and multiplication on \mathbb{Z}_n . Indeed, consider the addition modulo n $+_n$ and the multiplication modulo n \cdot_n defined by $[a]_n +_n [b]_n = [a+b]_n$ and $[a]_n \cdot_n [b]_n = [ab]_n$ for all $[a]_n, [b]_n \in \mathbb{Z}_n$. Then $+_n$ and \cdot_n are well defined binary operations on \mathbb{Z}_n .

Proof: We only prove here that \cdot_n is well defined, leaving the rest as an easy exercise. Let $[a_1]_n, [a_2]_n, [b_1]_n, [b_2]_n \in \mathbb{Z}_n$ be such that $[a_1]_n = [a_2]_n$ and $[b_1]_n = [b_2]_n$. (Want to prove that $[a_1]_n \cdot_n [b_1]_n = [a_2]_n \cdot_n [b_2]_n$). Then $a_1 - a_2 = n\upsilon$ and $b_1 - b_2 = n\varphi$ for some $\upsilon, \varphi \in \mathbb{Z}$. Now, note that $a_1 b_1 - a_2 b_2 = a_1 b_1 - a_2 b_1 + a_2 b_1 - a_2 b_2 = (a_1 - a_2)b_1 + a_2(b_1 - b_2) = n\upsilon b_1 + a_2 n\varphi = n(\upsilon b_1 + a_2 \varphi)$

So $n \mid a_1 b_1 - a_2 b_2$, implying that $[a_1 b_1]_n = [a_2 b_2]_n$. Hence, $[a_1]_n \cdot_n [b_1]_n = [a_2]_n \cdot_n [b_2]_n$ \square

Ex: The tables for $+_n$ and \cdot_n on \mathbb{Z}_n for $n=3$ are given by as follows:

$$\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$$

$+_3$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

\cdot_3	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Order Relations

Definition: Let A be a set and R be a relation on A .

(1) We say that R is a partial order on A if R is reflexive, antisymmetric and transitive. In this case we may also say that A is a partially ordered set or the pair (A, R) is a partially ordered set (\equiv "poset" for short).

(2) Let R be a partial order on A . We say that R is a total order (or linear order) if, for any $a, b \in A$, aRb or bRa . (i.e., any two elements of A are comparable) $((\forall a, b \in A) (aRb \vee bRa))$

(3) Let (A, R) be a poset, and B be a subset of A . We say that B is a chain in A if, for any $a, b \in B$, aRb or bRa . (i.e., R is a total order on B).

4) We usually use the notation \leq to denote partial orders. (Be careful here, \leq is just a notation, it is not the usual less than or equal to).

Ex: (1) (\mathbb{R}, \leq) is a poset, is a chain
the usual less than or equal to

For any $x, y, z \in \mathbb{R}$ note that $x \leq x$ (So \leq is reflexive)

$x \leq y$ and $y \leq x \Rightarrow x = y$ (So \leq is antisymm.)

$x \leq y$ and $y \leq z \Rightarrow x \leq z$ (So \leq is transitive)

$$x \leq y \text{ or } y \leq x$$

(2) Let A be a set. Then $(\mathcal{P}(A), \subseteq)$ is a poset

power set of A usual subset or equal

Let $x, y, z \in P(A)$. Note that $x \subseteq x$ (Reflexive)

$$X \subseteq Y \text{ and } Y \subseteq X \Rightarrow X=Y \text{ (Antisymmet.)}$$
$$X \subseteq Y \text{ and } Y \subseteq Z \Rightarrow X \subseteq Z \text{ (Transitive)}$$

If $|A| \geq 2$ then \subseteq is not a total order on $\mathcal{P}(A)$ (i.e. $\mathcal{P}(A)$ is not a

chain.

As $|A| > 1$, there are $x, y \in A$ such that $x \neq y$. Then $\{x\}, \{y\} \in P(A)$ but $\{x\} \not\subseteq \{y\}$ and $\{y\} \not\subseteq \{x\}$.

(3) $(\mathbb{N}, |)$ is a poset where, for any $a, b \in \mathbb{N}$, " $a|b$ " iff $b = ac \exists c \in \mathbb{N}$
↑
natural numbers "divides"

Let $x, y, z \in \mathbb{N}$.

As $x = x \cdot 1$, $x|x$. So $|$ is reflexive

Let $x|y$ and $y|x$. Then $y = xv \exists v \in \mathbb{N}$ and $x = yv \exists v \in \mathbb{N}$. Then $y = xv = (yv)v = y(vv)$. From $y = y(vv)$ we see that $y = 0$ or $vv = 1$. If $y = 0$ then $x = yv = 0$ too, and hence $x = y (= 0)$ in this case. If $vv = 1$ then $v = u = 1$ because $u, v \in \mathbb{N}$, and hence $x = yv = y$ in this case. As $x = y$ in both cases, $|$ is antisymmetric.

Let $x|y$ and $y|z$. Then $y = xm \exists m \in \mathbb{N}$ and $z = yn \exists n \in \mathbb{N}$. Then $z = yn = (xm)n = x(mn)$, so $x|z$. Hence, $|$ is transitive

As $|$ is reflexive, antisymmetric and transitive, $|$ is a partial order.

For instance, since $2 \nmid 3$ and $3 \nmid 2$, we see that $|$ is not a total order on \mathbb{N} .

Definition: Let (A, \leq) be a poset and $B \subseteq A$ a subset of A .

(1) An element b of B is called a smallest (or least, or minimum) element of B if $b \leq x$ for all $x \in B$.

(2) An element $b \in B$ is called a minimal element of B if there is no element $x \in B$ such that $x \leq b$ and $x \neq b$ (i.e., it is not the case that "there is an $x \in B$ such that $x \leq b$ and $x \neq b$ ")

$$\neg (\exists x \in B) (x \leq b \wedge x \neq b) \equiv (\forall x \in B) (x \leq b \rightarrow x = b)$$

(3) An element $b \in B$ is called a minimal element of B if, for all $x \in B$,

$x \leq b$ implies $x = b$

(4) An element $a \in A$ is called a lower bound of B (in A) if $a \leq x$ for all $x \in B$.

(5) We may define "greatest element of B , maximal element of B , upper bound of B " similarly:

An element $b \in B$ is called a (actually, the) greatest (or maximum) element of B if $x \leq b$ for all $x \in B$

An element $b \in B$ is called a maximal element of B if, for all $x \in B$, $b \leq x$ implies that $b = x$. (i.e., there is no element x of B such that $b \leq x$ and $b \neq x$).

An element $a \in A$ is called an upper bound of B if $x \leq a$ for all $x \in B$.

Fact: Let (A, \leq) be a poset and $B \subseteq A$ be a subset of A .

(1) If exists, smallest element of B is unique

(2) If exists, the smallest element of B is a minimal element of B .

But the converse is not true (i.e., there may be a minimal element of B which is not the smallest element of B).

(3) We have the similar facts for greatest and maximal element of B

Proof: Exercise \square

Ex: (1) $A = \{1, 2, 3, 4\}$. Consider the poset $(P(A), \subseteq)$, and the subset $\mathcal{F} = \{\{1\}, \{2\}, \{1, 2, 3\}\}$. Then,
 \nwarrow the usual subset or equal to

\mathcal{F} has no smallest element, $\{1\}$ and $\{2\}$ are minimal elements of \mathcal{F} , $\{1, 2, 3\}$ is the greatest element of \mathcal{F} and a maximal element of \mathcal{F} , \emptyset is a lower

of \mathcal{F} , A is an upper bound of \mathcal{F} , $\{1, 2, 3\}$ is an upper bound of \mathcal{F} .

Ex: In the poset $(\mathbb{Z}^+, |)$ consider the set $A = \{3, 4, 5, 6, 7, 8, 9\}$ where " $|$ " means "divides". A has no smallest element, $3, 4, 5, 7$ are all minimal elements of A , A has no greatest element, $5, 6, 7, 8, 9$ are all maximal elements of A , 1 is the unique lower bound of A , 360 is the smallest of the upper bounds of A .

Ex: Consider the poset $([0, 1], \leq)$ where $[0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ is an interval and " \leq " is the usual "less than or equal to". Consider the subset $B = \{1 - \frac{1}{n} \mid n \in \mathbb{Z}^+\}$ of $[0, 1]$. As \leq is a total order on \mathbb{R} , any subset, in particular B , is a chain in $([0, 1], \leq)$. Note that the upper bounds of B in \mathbb{R} are precisely real numbers ≥ 1 . In other words, B has no upper bound in $([0, 1], \leq)$ although it has in (\mathbb{R}, \leq) .

Theorem (Zorn's Lemma)

Let (A, \leq) be a nonempty poset. If every chain in A has an upper bound in A , then (A, \leq) has a maximal element.

We cannot prove Zorn's Lemma without assuming some axioms equivalent to it. Indeed, Zorn's Lemma is equivalent to Axiom of Choice. Although we will not have any application of it in this course, Zorn's Lemma is extremely important and it is used almost everywhere in which some kind of maximality occurs. Some classic applications of Zorn's Lemma are

- It is used to prove that every vector space has a basis.
- It is used to prove that every ring with 1 has a maximal ideal.
- It is used to prove that, for any sets A and B , either there is an injective function $A \rightarrow B$ or there is an injective function $B \rightarrow A$.

Definition: Let (A, \leq) be a poset. If every nonempty subset of A has a smallest element, then the partial order \leq is called a well order on A . In this case we may also say that the pair (A, \leq) is a well ordered set (or woset for short).

Ex: (1) If (A, \leq) is a woset then A is a chain (i.e., \leq is a total order on A).

Sol: Recalling the definition of a chain, we need to show that "for any $a, b \in A$, $a \leq b$ or $b \leq a$ ". Let $a, b \in A$. As $\{a, b\}$ is a nonempty subset of the woset (A, \leq) , the subset $\{a, b\}$ must have a smallest element. The smallest element of $\{a, b\}$ is either a or b . If it is a then $a \leq b$, and if it is b then $b \leq a$. Thus A is a chain. —

(2) Is (\mathbb{R}, \leq) a woset where \leq is the usual less than or equal to?

No. For instance the nonempty subset $(0, \infty) = \{x \in \mathbb{R} \mid x > 0\}$ of \mathbb{R} has no smallest element.

(3) Is (\mathbb{N}, \leq) a woset where \leq is the usual less than or equal to?

Yes. "Every nonempty subset of nonnegative integers has a smallest element". This intuitively clear result is known as the "well ordering principle" and it is to prove that "the proof by induction" is true.

(4) Let A be a set such that $|A| > 1$. Then $(\mathcal{P}(A), \subseteq)$ is not a poset where \subseteq is the usual subset or equal to.

As $|A| > 1$, there are two distinct elements a and b of A . Then the nonempty subset $\{\{a\}, \{b\}\}$ of $\mathcal{P}(A)$ has no smallest element. —

(5) Is (\mathbb{Z}, \leq) a woset where \leq is the usual less than or equal to?

No. For instance the nonempty subset $\mathbb{Z}^- = \{n \in \mathbb{Z} \mid n < 0\}$, the set of all negative integers, has no smallest element. —

(6) Define a relation \leq' on \mathbb{Z} as follows: For any $x, y \in \mathbb{Z}$

$$x \leq' y \text{ iff } |x| < |y| \text{ or } (|x| = |y| \text{ and } x \leq y)$$

where $<$ and \leq on the right are the usual less than and less than or equal to and $| \cdot |$ is the absolute value.

then (\mathbb{Z}, \leq') is a woset.

The proof of " \leq' is a partial order on \mathbb{Z} " is left as an exercise. We here show only that "a nonempty subset of (\mathbb{Z}, \leq') has a smallest element". Let A be a nonempty subset of \mathbb{Z} . Consider the set $B = \{|a| : a \in A\}$. Note that B is a nonempty subset of the nonnegative integers \mathbb{N} . So by the Well Ordering Principle B has the smallest element with respect to the usual less than or equal to. Let $b_0 \in B$ be the smallest element of B . Then $b_0 \leq b$ for all $b \in B$. By the definition of the set B there is an $a_0 \in A$ such that $b_0 = |a_0|$. If there is a negative $\tilde{a} \in A$ such that $|\tilde{a}| = b_0$, then let $a_0 \in A$ be negative. Thus, $a_0 \in A$ satisfies that " $|a_0| \leq |a|$ for all $a \in A$ ", and "if $|a_0| = |a|$ for an $a \in A$ then $a_0 \leq a$ " (because if a is negative then a_0 is negative too). So a_0 is the smallest element of A with respect to the partial order \leq' . Note that \leq' orders the elements of \mathbb{Z} as $0, -1, 1, -2, 2, -3, 3, \dots, -n, n, \dots$

We saw above that although \leq is not a well order on \mathbb{Z} , there is a well order \leq' on \mathbb{Z} . Indeed more is true. We won't give a proof of the following theorem which is equivalent to Axiom of Choice.

Theorem (Well Ordering Theorem)

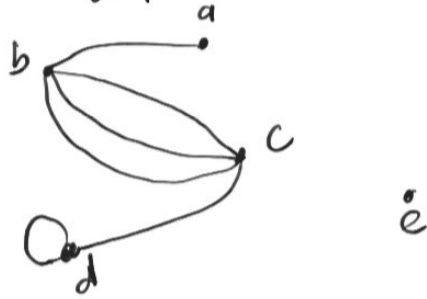
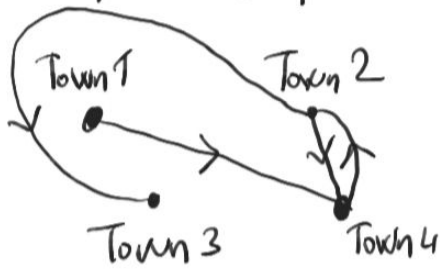
For any set A there is a partial order \leq on A such that (A, \leq) is a woset (In other words, any set can be well ordered).

Remark: The following are equivalent:

- (1) Axiom of Choice
- (2) Zorn's Lemma
- (3) Well Ordering Theorem.

Graph Theory

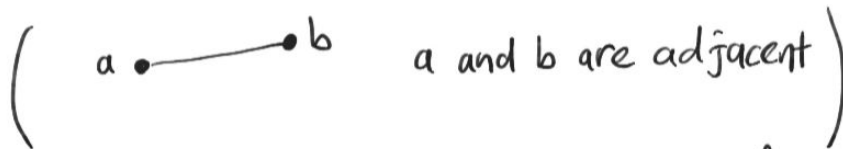
Intuitively "a picture with dots and lines (arcs) (directed or undirected) between some dots" is called a graph. Dots are called vertices, lines are called edges. If the lines have directions, the graph is called a directed graph or a digraph. If there are more than one lines between some dots, the graph is called a multigraph.



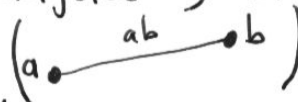
Definition: A graph G is a pair (V, E) where V is the set of vertices (In this course, assume that V is finite nonempty and E is finite!) and E is the set of edges. If the edges have directions, the graph is called directed or digraph. Each vertex is drawn as a dot and each edge is drawn as a line or curved line. If an edge has a direction we put an arrow on it.

Definition: Let $G = (V, E)$ be an undirected graph.

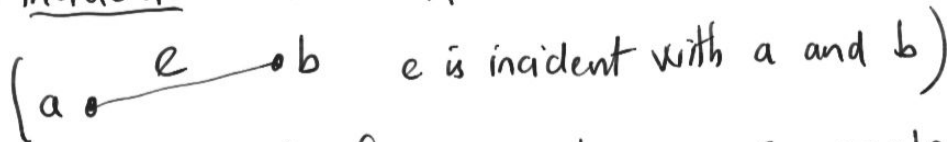
(1) Two vertices are called adjacent if there is an edge between them.



(2) If vertices a and b are adjacent, then ab or $a-b$ denotes an edge between a and b .



(3) If there is an edge e between vertices a and b , then we say that e is incident with a and b .

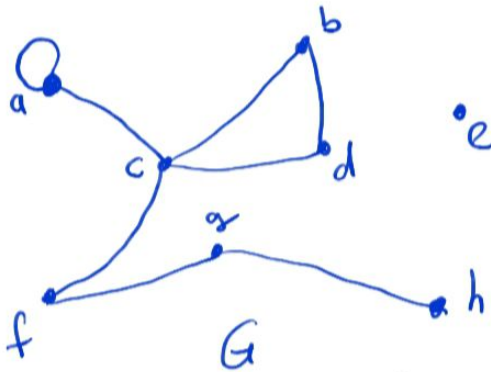


(4) Any edge of the form aa where a is a vertex (i.e., any edge connecting a to itself) is called a loop.



- (5) For any vertex v , the degree of v or the valence of v , denoted by $\deg(v)$, is defined to be the number of edges that are incident with v . Here a loop at v is considered as two incident edges for v .
- (6) G is called simple if G has no loops and G has no multiple edges.

Ex



$$\deg(a)=3, \deg(b)=2, \deg(c)=4, \\ \deg(d)=2, \deg(e)=0$$

$$V = \{a, b, c, d, e, f, g, h\}$$

$$E = \{aa, ac, bc, bd, cd, cf, \\ fg, gh\}$$

There is a loop at a
 b and d are adjacent
 e and h are not adjacent
 bc is incident with b and c
 G is not simple.

Definition: Let G be a digraph

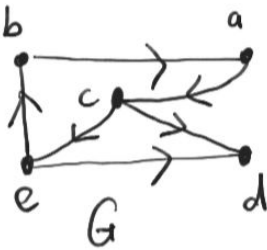
- (1) Edges of G are sometimes called arcs.
- (2) If there is an arc from a vertex a to a vertex b , we denote this by \vec{ab} (so that the arc starts at a and ends at b)



- (3) If there is an arc e from a vertex a to a vertex b , we say that a and b are adjacent, and that e is incident with a and b .
- (4) For any vertex \vec{v} , the incoming degree of v (or in-degree of v) is defined to be the number of arcs ending at v .
- (5) For any vertex \vec{v} , the outcoming degree of v (or out-degree of v) is defined to be the number of arcs starting at v .

(6) G is called simple if it has no loops and it has no multiple edges.

Ex:



$$V = \{a, b, c, d, e\}$$

$$E = \{ \vec{ba}, \vec{ac}, \vec{eb}, \vec{ce}, \vec{cd}, \vec{ed} \}$$

G is simple

$$\text{in-degree of } c = 1 \quad (\vec{ac})$$

$$\text{out-degree of } c = 2 \quad (\vec{ce}, \vec{cd})$$

Proposition: Let G be a digraph. Then

$$\left(\begin{array}{c} \text{The number of} \\ \text{arcs in } G \end{array} \right) = \left(\begin{array}{c} \text{The sum of} \\ \text{in-degrees of} \\ \text{vertices} \end{array} \right) = \left(\begin{array}{c} \text{The sum of} \\ \text{out-degrees of} \\ \text{vertices} \end{array} \right)$$

Proof: Let $V = \{v_1, v_2, \dots, v_n\}$ be the vertex set, and E be the edge set. For each $v_i \in V$ define

$$E_i = \{ \vec{v_i b} \in E \mid b \in V \} = \text{the set of arcs that starts at } v_i$$

Note that $|E_i| = \text{the out-degree of } v_i$, and $E_i \subseteq E$.

As each arc must begin at some vertex, $E = \bigcup_{i=1}^n E_i$. As an arc cannot begin at two distinct vertices, E_1, E_2, \dots, E_n are mutually disjoint.

$$\text{Hence, } |E| = \left| \bigcup_{i=1}^n E_i \right| = \sum_{i=1}^n |E_i|$$

↑
the number of
arcs in G .

↑
the sum of out-degrees
of vertices in G

Theorem: Let $G = (V, E)$ be an undirected graph. \square Then $\sum_{v \in V} \deg(v) = 2|E|$.
That is, the number of edges in G is exactly one-half of the sum of degrees of the vertices.

Proof: Consider the digraph constructed from G by replacing each edge with 2 opposite directed arcs (i.e., ab in G is replaced with \vec{ab} and \vec{ba} in H).



So, (the number of arcs in H) = $2 \times$ (the number of edges in G)

(the out-degree of v in H) = (the in-degree of v in H) = (the degree of v in G)

The result now follows from the previous proposition \square

Corollary: Let G be an undirected graph.

- (1) The sum of the degrees of the vertices is an even number.
- (2) The number of vertices of odd degree is even.

3) Let G be a simple graph with n vertices. Show that:

(a) The valence of every vertex is $\leq n - 1$. [Hint: No vertex is adjacent to itself.]

(b) If G has a vertex of valence 0, and $n \geq 2$, then G does *not* have a vertex of valence $n - 1$. [Hint: Can a vertex of valence $n - 1$ be adjacent to a vertex of valence 0?]

4) (a) What is the smallest possible valence of a vertex in a simple graph with 10 vertices?

(b) What is the largest possible valence of a vertex in a simple graph with 10 vertices?

7) Create a graph G whose vertices are the numbers $\{1, 2, \dots, n\}$, with an edge between x and y if and only if $x \neq y$ and $x \mid y$ or $y \mid x$. (See Definition 17.1 for the notation used here.) What vertices have valence 1?

8) (*harder*) Let G be a simple graph with at least 2 vertices. Show there are two different vertices of G that have the same valence.