

- 31.** a. Find an inverse for 210 modulo 13.
 b. Find a positive inverse for 210 modulo 13.
 c. Find a positive solution for the congruence $210x \equiv 8 \pmod{13}$.
- 32.** a. Find an inverse for 41 modulo 660.
 b. Find the least positive solution for the following congruence: $41x \equiv 125 \pmod{660}$.
- H 33.** Use Theorem 8.4.5 to prove that for all integers a , b , and c , if $\gcd(a, b) = 1$ and $a | c$ and $b | c$, then $ab | c$.
- 34.** Give a counterexample to show that the converse of exercise 33 is false.
- 35.** Corollary 8.4.7 guarantees the existence of an inverse modulo n for an integer a when a and n are relatively prime. Use Euclid's lemma to prove that the inverse is unique modulo n . In other words, show that any two integers whose product with a is congruent to 1 modulo n are congruent to each other modulo n .

In 36, 37, 39, and 40, use the RSA cipher with public key $n = 713 = 23 \cdot 31$ and $e = 43$. In 36 and 37, encode the messages into their numeric equivalents and encrypt them. In 39 and 40, decrypt the given ciphertext and find the original messages.

36. HELP 37. COME

38. Find the least positive inverse for 43 modulo 660.
- 39.** 675 089 089 048
40. 028 018 675 129

- H 41. a.** Use mathematical induction and Euclid's lemma to prove that for all positive integers s , if p and q_1, q_2, \dots, q_s are prime numbers and $p | q_1 q_2 \cdots q_s$, then $p = q_i$ for some i with $1 \leq i \leq s$.

Answers for Test Yourself

- three places in the alphabet to the right of the letter, with X wrapped around to A , Y to B , and Z to C
- $a \equiv b \pmod{n}$; $a = b + kn$ for some integer k ; a and b have the same nonnegative remainder when divided by n ; $a \bmod n = b \bmod n$
- $(c+d) \pmod{n}$; $(c-d) \pmod{n}$; $(cd) \pmod{n}$; $c^m \pmod{n}$
- sum of powers of 2
- version of the Euclidean
- a linear combination of a and n
- $C = M^e \bmod pq$; $M = C^d \bmod pq$; d is a positive inverse for e modulo $(p-1)(q-1)$
- $a | b$
- $a^{p-1} \equiv 1 \pmod{p}$
- $M^{ed} \bmod pq$

8.5 Partial Order Relations

There is no branch of mathematics, however abstract, which may not some day be applied to phenomena of the real world. — Nicolai Ivanovich Lobachevsky, 1792–1856

In order to obtain a degree in computer science at a certain university, a student must take a specified set of required courses, some of which must be completed before others can be started. Given the prerequisite structure of the program, one might ask what is the least number of school terms needed to fulfill the degree requirements, or what is the maximum number of courses that can be taken in the same term, or whether there is a sequence in which a part-time student can take the courses one per term. Later in this section, we will show how representing the prerequisite structure of the program as a partial order relation makes it relatively easy to answer such questions.

- b. The uniqueness part of the unique factorization theorem for the integers says that given any integer n , if

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

for some positive integers r and s and prime numbers $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$, then $r = s$ and $p_i = q_i$ for all integers i with $1 \leq i \leq r$.

Use the result of part (a) to fill in the details of the following sketch of a proof: Suppose that n is an integer with two different prime factorizations: $n = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_u$. All the prime factors that appear on both sides can be cancelled (as many times as they appear on both sides) to arrive at the situation where $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, $p_1 \leq p_2 \leq \cdots \leq p_r$, $q_1 \leq q_2 \leq \cdots \leq q_s$, and $p_i \neq q_j$ for any integers i and j . Then use part (a) to deduce a contradiction, and so the prime factorization of n is unique except, possibly, for the order in which the prime factors are written.

42. According to Fermat's little theorem, if p is a prime number and a and p are relatively prime, then $a^{p-1} \equiv 1 \pmod{p}$. Verify that this theorem gives correct results for
a. $a = 15$ and $p = 7$ **b.** $a = 8$ and $p = 11$
43. Fermat's little theorem can be used to show that a number is not prime by finding a number a relatively prime to p with the property that $a^{p-1} \not\equiv 1 \pmod{p}$. However, it cannot be used to show that a number *is* prime. Find an example to illustrate this fact. That is, find integers a and p such that a and p are relatively prime and $a^{p-1} \equiv 1 \pmod{p}$ but p is not prime.

Antisymmetry

In Section 8.2 we defined three properties of relations: reflexivity, symmetry, and transitivity. A fourth property of relations is called *antisymmetry*. In terms of the arrow diagram of a relation, saying that a relation is antisymmetric is the same as saying that whenever there is an arrow going from one element to another *distinct* element, there is *not* an arrow going back from the second to the first.

• Definition

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 $a = b$.

By taking the negation of the definition, you can see that a relation R is **not antisymmetric** if, and only if,

there are elements a and b in A such that $a R b$ and $b R a$ but $a \neq b$.

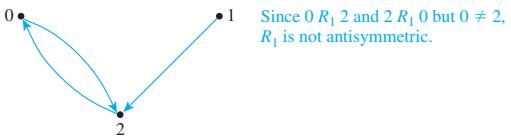
Example 8.5.1 Testing for Antisymmetry of Finite Relations

Let R_1 and R_2 be the relations on $\{0, 1, 2\}$ defined as follows: Draw the directed graphs for R_1 and R_2 and indicate which relations are antisymmetric.

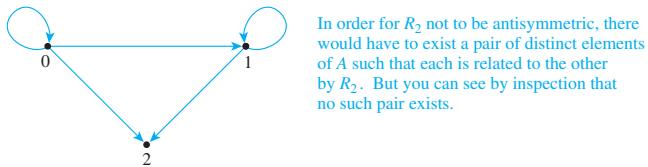
- $R_1 = \{(0, 2), (1, 2), (2, 0)\}$
- $R_2 = \{(0, 0), (0, 1), (0, 2), (1, 1), (1, 2)\}$

Solution

- a. R_1 is not antisymmetric.



- b. R_2 is antisymmetric.



Example 8.5.2 Testing for Antisymmetry of “Divides” Relations

Let R_1 be the “divides” relation on the set of all positive integers, and let R_2 be the “divides” relation on the set of all integers.

For all $a, b \in \mathbb{Z}^+$, $a R_1 b \Leftrightarrow a b$.	For all $a, b \in \mathbb{Z}$, $a R_2 b \Leftrightarrow a b$.
---	---

- Is R_1 antisymmetric? Prove or give a counterexample.
- Is R_2 antisymmetric? Prove or give a counterexample.

Solution

- R_1 is antisymmetric.

Proof:

Suppose a and b are positive integers such that $a R_1 b$ and $b R_1 a$. [We must show that $a = b$.] By definition of R_1 , $a | b$ and $b | a$. Thus, by definition of divides, there are integers k_1 and k_2 with $b = k_1a$ and $a = k_2b$. It follows that

$$b = k_1a = k_1(k_2b) = (k_1k_2)b.$$

Dividing both sides by b gives

$$k_1k_2 = 1.$$

Now since a and b are both integers k_1 and k_2 are both positive integers also. But the only product of two positive integers that equals 1 is $1 \cdot 1$. Thus

$$k_1 = k_2 = 1$$

and so

$$a = k_2b = 1 \cdot b = b.$$

[This is what was to be shown.]

- R_2 is not antisymmetric.

Counterexample:

Let $a = 2$ and $b = -2$. Then $a | b$ [since $-2 = (-1) \cdot 2$] and $b | a$ [since $2 = (-1)(-2)$]. Hence $a R_2 b$ and $b R_2 a$ but $a \neq b$. ■

Example 8.5.2 illustrates the fact that a relation may be antisymmetric on a subset of a set but not antisymmetric on the set itself.

Partial Order Relations

A relation that is reflexive, antisymmetric, and transitive is called a *partial order*.

• **Definition**

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

Two fundamental partial order relations are the “less than or equal to” relation on a set of real numbers and the “subset” relation on a set of sets. These can be thought of as models, or paradigms, for general partial order relations.

Example 8.5.3 The “Subset” Relation

Let \mathcal{A} be any collection of sets and define the “subset” relation, \subseteq , on \mathcal{A} as follows: For all $U, V \in \mathcal{A}$,

$$U \subseteq V \Leftrightarrow \text{for all } x, \text{ if } x \in U \text{ then } x \in V.$$

By an argument almost identical to that of the solution for exercise 23 of Section 8.2, \subseteq is reflexive and transitive. Finish the proof that \subseteq is a partial order relation by proving that \subseteq is antisymmetric.

Solution For \subseteq to be antisymmetric means that for all sets U and V in \mathcal{A} if $U \subseteq V$ and $V \subseteq U$ then $U = V$. But this is true by definition of equality of sets. ■

Example 8.5.4 A “Divides” Relation on a Set of Positive Integers

Let $|$ be the “divides” relation on a set A of positive integers. That is, for all $a, b \in A$,

$$a | b \Leftrightarrow b = ka \text{ for some integer } k.$$

Prove that $|$ is a partial order relation on A .

Solution

$|$ is reflexive: [We must show that for all $a \in A$, $a | a$.] Suppose $a \in A$. Then $a = 1 \cdot a$, so $a | a$ by definition of divisibility.

$|$ is antisymmetric: [We must show that for all $a, b \in A$, if $a | b$ and $b | a$ then $a = b$.] The proof of this is virtually identical to that of Example 8.5.2(a).

$|$ is transitive: To show transitivity means to show that for all $a, b, c \in A$, if $a | b$ and $b | c$ then $a | c$. But this was proved as Theorem 4.3.3.

Since $|$ is reflexive, antisymmetric, and transitive, $|$ is a partial order relation on A . ■

Example 8.5.5 The “Less Than or Equal to” Relation

Let S be a set of real numbers and define the “less than or equal to” relation, \leq , on S as follows: For all real numbers x and y in S ,

$$x \leq y \Leftrightarrow x < y \text{ or } x = y.$$

Show that \leq is a partial order relation.

Solution

\leq is reflexive: For \leq to be reflexive means that $x \leq x$ for all real numbers x in S . But $x \leq x$ means that $x < x$ or $x = x$, and $x = x$ is always true.

\leq is antisymmetric: For \leq to be antisymmetric means that for all real numbers x and y in S , if $x \leq y$ and $y \leq x$ then $x = y$. This follows immediately from the definition of \leq and the trichotomy property (see Appendix A, T17), which says that given any real numbers, x and y , exactly one of the following holds: $x < y$ or $x = y$ or $x > y$.

\leq is transitive: For \leq to be transitive means that for all real numbers x, y , and z in S if $x \leq y$ and $y \leq z$ then $x \leq z$. This follows from the definition of \leq and the transitivity property of order (see Appendix A, T18), which says that given any real numbers x, y , and z , if $x < y$ and $y < z$ then $x < z$.

Because \leq is reflexive, antisymmetric, and transitive, it is a partial order relation. ■

• Notation

Because of the special paradigmatic role played by the \leq relation in the study of partial order relations, the symbol \leq is often used to refer to a general partial order relation, and the notation $x \leq y$ is read “ x is less than or equal to y ” or “ y is greater than or equal to x .”

Lexicographic Order

To figure out which of two words comes first in an English dictionary, you compare their letters one by one from left to right. If all letters have been the same to a certain point and one word runs out of letters, that word comes first in the dictionary. For example, *play* comes before *playhouse*. If all letters up to a certain point are the same and the next letters differ, then the word whose next letter is located earlier in the alphabet comes first in the dictionary. For instance, *playhouse* comes before *playmate*.

More generally, if A is any set with a partial order relation, then a *dictionary* or *lexicographic* order can be defined on a set of strings over A as indicated in the following theorem.

Theorem 8.5.1

Let A be a set with a partial order relation R , and let S be a set of strings over A . Define a relation \preceq on S as follows:

For any two strings in S , $a_1a_2 \cdots a_m$ and $b_1b_2 \cdots b_n$, where m and n are positive integers,

1. If $m \leq n$ and $a_i = b_i$ for all $i = 1, 2, \dots, m$, then

$$a_1a_2 \cdots a_m \preceq b_1b_2 \cdots b_n.$$

2. If for some integer k with $k \leq m$, $k \leq n$, and $k \geq 1$, $a_i = b_i$ for all $i = 1, 2, \dots, k - 1$, and $a_k \neq b_k$, but $a_k R b_k$ then

$$a_1a_2 \cdots a_m \preceq b_1b_2 \cdots b_n.$$

3. If ϵ is the null string and s is any string in S , then $\epsilon \preceq s$.

If no strings are related other than by these three conditions, then \preceq is a partial order relation.

The proof of Theorem 8.5.1 is technical but straightforward. It is left for the exercises.

• Definition

The partial order relation of Theorem 8.5.1 is called the **lexicographic order for S** that corresponds to the partial order R on A .

Example 8.5.6 A Lexicographic Order

Let $A = \{x, y\}$ and let R be the following partial order relation on A :

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

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

- Is $x \preceq xx?$ $x \preceq xy?$ $xx \preceq xxx?$ $yxy \preceq yxyxxx?$
- Is $x \preceq y?$ $xx \preceq yxy?$ $xxxy \preceq xy?$ $yxyxxyy \preceq yxyxy?$
- Is $\epsilon \preceq x?$ $\epsilon \preceq xy?$ $\epsilon \preceq yyxy?$

Solution

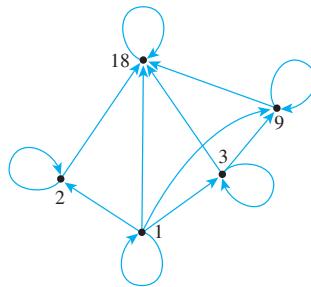
- Yes in all cases, by property (1) of the definition of \preceq .
- Yes in all cases, by property (2) of the definition of \preceq .
- Yes in all cases, by property (3) of the definition of \preceq . ■

Hasse Diagrams

Let $A = \{1, 2, 3, 9, 18\}$ and consider the “divides” relation on A : For all $a, b \in A$,

$$a | b \Leftrightarrow b = ka \text{ for some integer } k.$$

The directed graph of this relation has the following appearance:

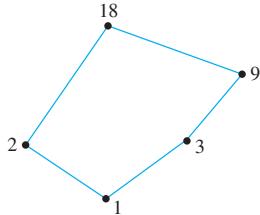


Note that there is a loop at every vertex, all other arrows point in the same direction (upward), and any time there is an arrow from one point to a second and from the second point to a third, there is an arrow from the first point to the third. Given any partial order relation defined on a finite set, it is possible to draw the directed graph in such a way that all of these properties are satisfied. This makes it possible to associate a somewhat simpler graph, called a **Hasse diagram** (after Helmut Hasse, a twentieth-century German number theorist), with a partial order relation defined on a finite set. To obtain a Hasse diagram, proceed as follows:

Start with a directed graph of the relation, placing vertices on the page so that all arrows point upward. Then eliminate

- the loops at all the vertices,
- all arrows whose existence is implied by the transitive property,
- the direction indicators on the arrows.

For the relation given previously, the Hasse diagram is as follows:



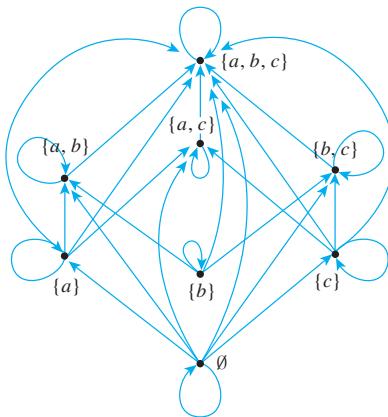
Example 8.5.7 Constructing a Hasse Diagram

Consider the “subset” relation, \subseteq , on the set $\mathcal{P}(\{a, b, c\})$. That is, for all sets U and V in $\mathcal{P}(\{a, b, c\})$,

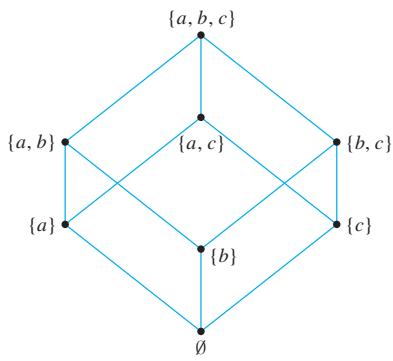
$$U \subseteq V \Leftrightarrow \forall x, \text{ if } x \in U \text{ then } x \in V.$$

Construct the Hasse diagram for this relation.

Solution Draw the directed graph of the relation in such a way that all arrows except loops point upward.



Then strip away all loops, unnecessary arrows, and direction indicators to obtain the Hasse diagram.

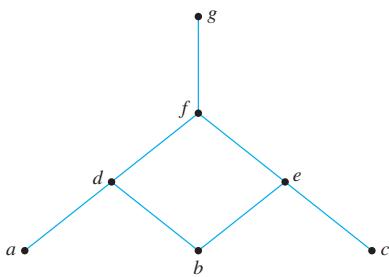


To recover the directed graph of a relation from the Hasse diagram, just reverse the instructions given previously, using the knowledge that the original directed graph was sketched so that all arrows pointed upward:

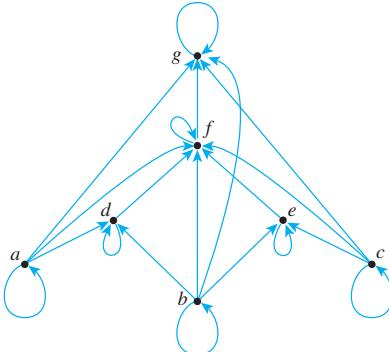
1. Reinsert the direction markers on the arrows making all arrows point upward.
2. Add loops at each vertex.
3. For each sequence of arrows from one point to a second and from that second point to a third, add an arrow from the first point to the third.

Example 8.5.8 Obtaining the Directed Graph of a Partial Order Relation from the Hasse Diagram of the Relation

A partial order relation R has the following Hasse diagram. Find the directed graph of R .



Solution



Partially and Totally Ordered Sets

Given any two real numbers x and y , either $x \leq y$ or $y \leq x$. In a situation like this, the elements x and y are said to be *comparable*. On the other hand, given two subsets A and B of $\{a, b, c\}$, it may be the case that neither $A \subseteq B$ nor $B \subseteq A$. For instance, let $A = \{a, b\}$ and $B = \{b, c\}$. Then $A \not\subseteq B$ and $B \not\subseteq A$. In such a case, A and B are said to be *noncomparable*.

• Definition

Suppose \preceq is a partial order relation on a set A . Elements a and b of A are said to be **comparable** if, and only if, either $a \preceq b$ or $b \preceq a$. Otherwise, a and b are called **noncomparable**.

When all the elements of a partial order relation are comparable, the relation is called a *total order*.

• **Definition**

If R is a partial order relation on a set A , and for any two elements a and b in A either $a R b$ or $b R a$, then R is a **total order relation** on A .

Both the “less than or equal to” relation on sets of real numbers and the lexicographic order of the set of words in a dictionary are total order relations. Note that the Hasse diagram for a total order relation can be drawn as a single vertical “chain.”

Many important partial order relations have elements that are not comparable and are, therefore, not total order relations. For instance, the subset relation on $\mathcal{P}(\{a, b, c\})$ is not a total order relation because, as shown previously, the subsets $\{a, b\}$ and $\{a, c\}$ of $\{a, b, c\}$ are not comparable. In addition, a “divides” relation is not a total order relation unless the elements are all powers of a single integer. (See exercise 21 at the end of this section.)

A set A is called a **partially ordered set** (or **poset**) with respect to a relation \preceq if, and only if, \preceq is a partial order relation on A . For instance, the set of real numbers is a partially ordered set with respect to the “less than or equal to” relation \leq , and a set of sets is partially ordered with respect to the “subset” relation \subseteq . It is entirely straightforward to show that *any subset of a partially ordered set is partially ordered*. (See exercise 35 at the end of this section.) This, of course, assumes the “same definition” for the relation on the subset as for the set as a whole. A set A is called a **totally ordered set** with respect to a relation \preceq if, and only if, A is partially ordered with respect to \preceq and \preceq is a total order.

A set that is partially ordered but not totally ordered may have totally ordered subsets. Such subsets are called *chains*.

• **Definition**

Let A be a set that is partially ordered with respect to a relation \preceq . A subset B of A is called a **chain** if, and only if, the elements in each pair of elements in B is comparable. In other words, $a \preceq b$ or $b \preceq a$ for all a and b in A . The **length of a chain** is one less than the number of elements in the chain.

Observe that if B is a chain in A , then B is a totally ordered set with respect to the “restriction” of \preceq to B .

Example 8.5.9 A Chain of Subsets

The set $\mathcal{P}(\{a, b, c\})$ is partially ordered with respect to the subset relation. Find a chain of length 3 in $\mathcal{P}(\{a, b, c\})$.

Solution Since $\emptyset \subseteq \{a\} \subseteq \{a, b\} \subseteq \{a, b, c\}$, the set

$$S = \{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}\}$$

is a chain of length 3 in $\mathcal{P}(\{a, b, c\})$. ■

In exercise 39 at the end of this section, you are asked to show that a set that is partially ordered with respect to a relation \preceq is totally ordered with respect to \preceq if, and only if, it is a chain.

A *maximal element* in a partially ordered set is an element that is greater than or equal to every element to which it is comparable. (There may be many elements to which it is *not* comparable.) A *greatest element* in a partially ordered set is an element that is greater than or equal to every element in the set (so it is comparable to every element in the set). Minimal and least elements are defined similarly.

• Definition

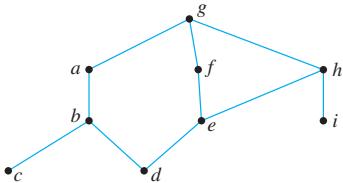
Let a set A be partially ordered with respect to a relation \leq .

1. An element a in A is called a **maximal element of A** if, and only if, for all b in A , either $b \leq a$ or b and a are not comparable.
2. An element a in A is called a **greatest element of A** if, and only if, for all b in A , $b \leq a$.
3. An element a in A is called a **minimal element of A** if, and only if, for all b in A , either $a \leq b$ or b and a are not comparable.
4. An element a in A is called a **least element of A** if, and only if, for all b in A , $a \leq b$.

A greatest element is maximal, but a maximal element need not be a greatest element. However, every finite subset of a totally ordered set has both a least element and a greatest element. (See exercise 40 at the end of the section.) Similarly, a least element is minimal, but a minimal element need not be a least element. Furthermore, a set that is partially ordered with respect to a relation can have at most one greatest element and one least element (see exercise 42 at the end of the section), but it may have more than one maximal or minimal element. The next example illustrates some of these facts.

Example 8.5.10 Maximal, Minimal, Greatest, and Least Elements

Let $A = \{a, b, c, d, e, f, g, h, i\}$ have the partial ordering \leq defined by the following Hasse diagram. Find all maximal, minimal, greatest, and least elements of A .



Solution There is just one maximal element, g , which is also the greatest element. The minimal elements are c , d , and i , and there is no least element. ■

Topological Sorting

Is it possible to input the sets of $\mathcal{P}(\{a, b, c\})$ into a computer in a way that is *compatible* with the subset relation \subseteq in the sense that if set U is a subset of set V , then U is input before V ? The answer, as it turns out, is yes. For instance, the following input order satisfies the given condition:

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}.$$

Another input order that satisfies the condition is

$$\emptyset, \{a\}, \{b\}, \{a, b\}, \{c\}, \{b, c\}, \{a, c\}, \{a, b, c\}.$$

• Definition

Given partial order relations \leq and \leq' on a set A , \leq' is **compatible** with \leq if, and only if, for all a and b in A , if $a \leq b$ then $a \leq' b$.

Given an arbitrary partial order relation \leq on a set A , is there a total order \leq' on A that is compatible with \leq ? If the set on which the partial order is defined is finite, then the answer is yes. A total order that is compatible with a given order is called a *topological sorting*.

• Definition

Given partial order relations \leq and \leq' on a set A , \leq' is a **topological sorting** for \leq if, and only if, \leq' is a total order that is compatible with \leq .

The construction of a topological sorting for a general finite partially ordered set is based on the fact that *any partially ordered set that is finite and nonempty has a minimal element*. (See exercise 41 at the end of the section.) To create a total order for a partially ordered set, simply pick any minimal element and make it number one. Then consider the set obtained when this element is removed. Since the new set is a subset of a partially ordered set, it is partially ordered. If it is empty, stop the process. If not, pick a minimal element from it and call that element number two. Then consider the set obtained when this element also is removed. If this set is empty, stop the process. If not, pick a minimal element and call it number three. Continue in this way until all the elements of the set have been used up.

Here is a somewhat more formal version of the algorithm:

Constructing a Topological Sorting

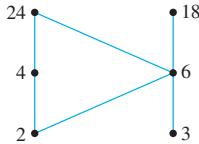
Let \leq be a partial order relation on a nonempty finite set A . To construct a topological sorting,

1. Pick any minimal element x in A . [Such an element exists since A is nonempty.]
2. Set $A' := A - \{x\}$.
3. Repeat steps a–c while $A' \neq \emptyset$.
 - a. Pick any minimal element y in A' .
 - b. Define $x \leq' y$.
 - c. Set $A' := A' - \{y\}$ and $x := y$.

[Completion of steps 1–3 of this algorithm gives enough information to construct the Hasse diagram for the total ordering \leq' . We have already shown how to use the Hasse diagram to obtain a complete directed graph for a relation.]

Example 8.5.11 A Topological Sorting

Consider the set $A = \{2, 3, 4, 6, 18, 24\}$ ordered by the “divides” relation $|$. The Hasse diagram of this relation is the following:

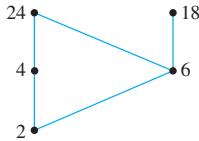


The ordinary “less than or equal to” relation \leq on this set is a topological sorting for it since for positive integers a and b , if $a | b$ then $a \leq b$. Find another topological sorting for this set.

Solution The set has two minimal elements: 2 and 3. Either one may be chosen; say you pick 3. The beginning of the total order is

total order: 3.

Set $A' = A - \{3\}$. You can indicate this by removing 3 from the Hasse diagram as shown below.



Next choose minimal element from $A' - \{3\}$. Only 2 is minimal, so you must pick it. The total order thus far is

total order: $3 \leq 2$.

Set $A' = (A - \{3\}) - \{2\} = A - \{3, 2\}$. You can indicate this by removing 2 from the Hasse diagram, as is shown below.



Choose a minimal element from $A' - \{3, 2\}$. Again you have two choices: 4 and 6. Say you pick 6. The total order for the elements chosen thus far is

total order: $3 \leq 2 \leq 6$.

You continue in this way until every element of A has been picked. One possible sequence of choices gives

total order: $3 \leq 2 \leq 6 \leq 18 \leq 4 \leq 24$.

You can verify that this order is compatible with the “divides” partial order by checking that for each pair of elements a and b in A such that $a | b$, then $a \leq b$. Note that it is *not* the case that if $a \leq b$ then $a | b$. ■

An Application

To return to the example that introduced this section, note that the following defines a partial order relation on the set of courses required for a university degree: For all required courses x and y ,

$$x \preceq y \Leftrightarrow x = y \text{ or } x \text{ is a prerequisite for } y$$

If the Hasse diagram for the relation is drawn, then the questions raised at the beginning of this section can be answered easily. For instance, consider the Hasse diagram for the requirements at a particular university, which is shown in Figure 8.5.1.

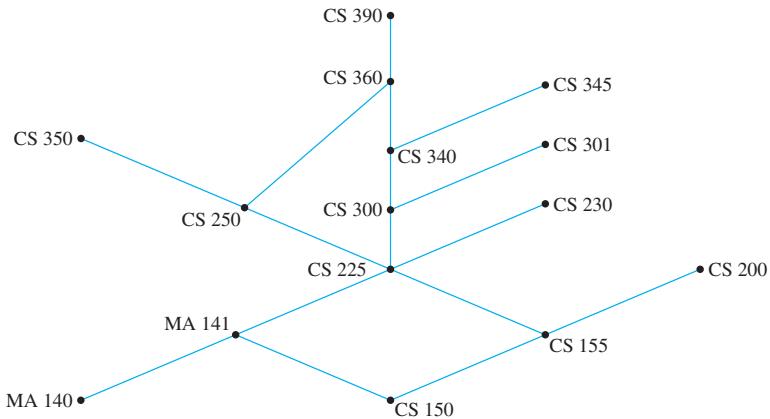


Figure 8.5.1

The minimum number of school terms needed to complete the requirements is the size of a longest chain, which is 7 (150, 155, 225, 300, 340, 360, 390, for example). The maximum number of courses that could be taken in the same term (assuming the university allows it) is the maximum number of noncomparable courses, which is 6 (350, 360, 345, 301, 230, 200, for example). A part-time student could take the courses in a sequence determined by constructing a topological sorting for the set. (One such sorting is 140, 150, 141, 155, 200, 225, 230, 300, 250, 301, 340, 345, 350, 360, 390. There are many others.)

PERT and CPM

Two important and widely used applications of partial order relations are **PERT** (Program Evaluation and Review Technique) and **CPM** (Critical Path Method). These techniques came into being in the 1950s as planners came to grips with the complexities of scheduling the individual activities needed to complete very large projects, and although they are very similar, their developments were independent. PERT was developed by the U.S. Navy to help organize the construction of the Polaris submarine, and CPM was developed by the E. I. Du Pont de Nemours company for scheduling chemical plant maintenance. Here is a somewhat simplified example of the way the techniques work.

Example 8.5.12 A Job Scheduling Problem

At an automobile assembly plant, the job of assembling an automobile can be broken down into these tasks:

1. Build frame.
2. Install engine, power train components, gas tank.
3. Install brakes, wheels, tires.
4. Install dashboard, floor, seats.
5. Install electrical lines.
6. Install gas lines.
7. Install brake lines.
8. Attach body panels to frame.
9. Paint body.

Certain of these tasks can be carried out at the same time, whereas some cannot be started until other tasks are finished. Table 8.5.1 summarizes the order in which tasks can be performed and the time required to perform each task.

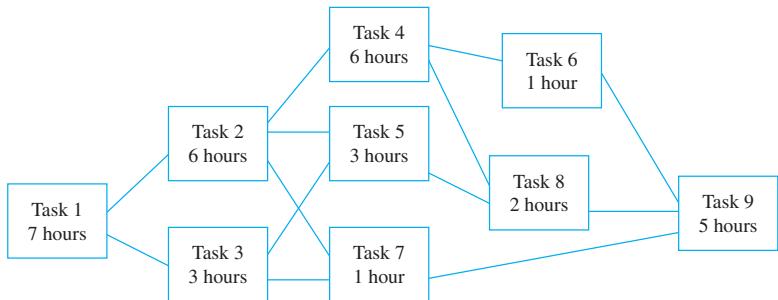
Table 8.5.1

Task	Immediately Preceding Tasks	Time Needed to Perform Task
1		7 hours
2	1	6 hours
3	1	3 hours
4	2	6 hours
5	2, 3	3 hours
6	4	1 hour
7	2, 3	1 hour
8	4, 5	2 hours
9	6, 7, 8	5 hours

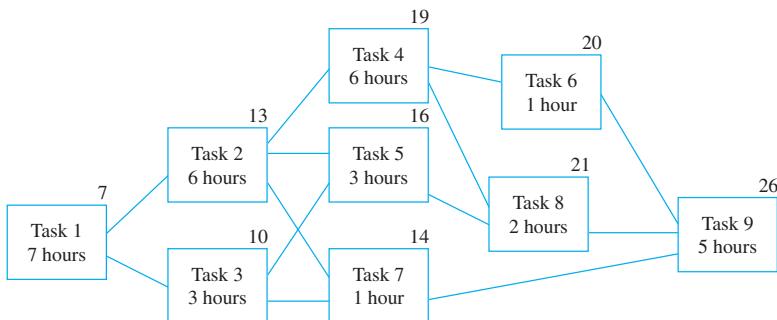
Let T be the set of all tasks, and consider the partial order relation \preceq defined on T as follows: For all tasks x and y in T ,

$$x \preceq y \Leftrightarrow x = y \text{ or } x \text{ precedes } y.$$

If the Hasse diagram of this relation is turned sideways (as is customary in PERT and CPM analysis), it has the appearance shown below.



What is the minimum time required to assemble a car? You can determine this by working from left to right across the diagram, noting for each task (say, just above the box representing that task) the minimum time needed to complete that task starting from the beginning of the assembly process. For instance, you can put a 7 above the box for task 1 because task 1 requires 7 hours. Task 2 requires completion of task 1 (7 hours) plus 6 hours for itself, so the minimum time required to complete task 2, starting at the beginning of the assembly process, is $7 + 6 = 13$ hours. You can put a 13 above the box for task 2. Similarly, you can put a 10 above the box for task 3 because $7 + 3 = 10$. Now consider what number you should write above the box for task 5. The minimum times to complete tasks 2 and 3, starting from the beginning of the assembly process, are 13 and 10 hours respectively. Since *both* tasks must be completed before task 5 can be started, the minimum time to complete task 5, starting from the beginning, is the time needed for task 5 itself (3 hours) plus the *maximum* of the times to complete tasks 2 and 3 (13 hours), and this equals $3 + 13 = 16$ hours. Thus you should place the number 16 above the box for task 5. The same reasoning leads you to place a 14 above the box for task 7. Similarly, you can place a 19 above the box for task 4, a 20 above the box for task 6, a 21 above the box for task 8, and a 26 above the box for task 9, as shown below.



This analysis shows that at least 26 hours are required to complete task 9 starting from the beginning of the assembly process. When task 9 is finished, the assembly is complete, so 26 hours is the minimum time needed to accomplish the whole process.

Note that the minimum time required to complete tasks 1, 2, 4, 8, and 9 in sequence is exactly 26 hours. This means that a delay in performing any one of these tasks causes a delay in the total time required for assembly of the car. For this reason, the path through tasks 1, 2, 4, 8, and 9 is called a **critical path**.

Test Yourself

- For a relation R on a set A to be antisymmetric means that _____.
- To show that a relation R on an infinite set A is antisymmetric, you suppose that _____ and you show that _____.
- To show that a relation R on a set A is not antisymmetric, you _____.
- To construct a Hasse diagram for a partial order relation, you start with a directed graph of the relation in which all arrows point upward and you eliminate _____, _____, and _____.
- If A is a set that is partially ordered with respect to a relation \leq and if a and b are elements of A , we say that a and b are comparable if, and only if, _____ or _____.
- A relation \leq on a set A is a total order if, and only if, _____.
- If A is a set that is partially ordered with respect to a relation \leq , and if B is a subset of A , then B is a chain if, and only if, for all a and b in B , _____.

8. Let A be a set that is partially ordered with respect to a relation \leq , and let a be an element of A .
- a is maximal if, and only if, _____.
 - a is a greatest element of A if, and only if, _____.
 - a is minimal if, and only if, _____.
 - a is a least element of A if, and only if, _____.

Exercise Set 8.5

1. Each of the following is a relation on $\{0, 1, 2, 3\}$. Draw directed graphs for each relation, and indicate which relations are antisymmetric.
- $R_1 = \{(0, 0), (0, 2), (1, 0), (1, 3), (2, 2), (3, 0), (3, 1)\}$
 - $R_2 = \{(0, 1), (0, 2), (1, 1), (1, 2), (1, 3), (2, 2), (3, 2)\}$
 - $R_3 = \{(0, 0), (0, 3), (1, 0), (1, 3), (2, 2), (3, 3), (3, 2)\}$
 - $R_4 = \{(0, 0), (1, 0), (1, 2), (1, 3), (2, 0), (2, 1), (3, 2), (3, 0)\}$
2. Let P be the set of all people in the world and define a relation R on P as follows: For all $x, y \in P$,
- $$x R y \Leftrightarrow x \text{ is no older than } y.$$
- Is R antisymmetric? Prove or give a counterexample.
3. Let S be the set of all strings of a 's and b 's. Define a relation R on S as follows: For all $t \in S$,
- $$s R t \Leftrightarrow l(s) \leq l(t),$$
- where $l(x)$ denotes the length of a string x . Is R antisymmetric? Prove or give a counterexample.
4. Let R be the “less than” relation on the set \mathbf{R} of all real numbers: For all $x, y \in \mathbf{R}$,
- $$x R y \Leftrightarrow x < y.$$
- Is R antisymmetric? Prove or give a counterexample.
5. Let \mathbf{R} be the set of all real numbers and define a relation R on $\mathbf{R} \times \mathbf{R}$ as follows: For all (a, b) and (c, d) in $\mathbf{R} \times \mathbf{R}$,
- $$(a, b) R (c, d) \Leftrightarrow \text{either } a < c \text{ or both } a = c \text{ and } b \leq d.$$
- Is R a partial order relation? Prove or give a counterexample.
6. Let P be the set of all people who have ever lived and define a relation R on P as follows: For all $r, s \in P$,
- $$r R s \Leftrightarrow r \text{ is an ancestor of } s \text{ or } r = s.$$
- Is R a partial order relation? Prove or give a counterexample.
7. Define a relation R on the set \mathbf{Z} of all integers as follows: For all $m, n \in \mathbf{Z}$,
- $$m R n \Leftrightarrow \text{every prime factor of } m \text{ is a prime factor of } n.$$
- Is R a partial order relation? Prove or give a counterexample.
9. Given a set A that is partially ordered with respect to a relation \leq , the relation \leq' is a topological sorting for \leq , if, and only if, \leq' is a _____ and for all a and b in A if $a \leq b$ then _____.
10. PERT and CPM are used to produce efficient _____.
8. Define a relation R on the set \mathbf{Z} of all integers as follows: For all $m, n \in \mathbf{Z}$,
- $$m R n \Leftrightarrow m + n \text{ is even.}$$
- Is R a partial order relation? Prove or give a counterexample.
9. Define a relation R on the set of all real numbers \mathbf{R} as follows: For all $x, y \in \mathbf{R}$,
- $$x R y \Leftrightarrow x^2 \leq y^2.$$
- Is R a partial order relation? Prove or give a counterexample.
10. Suppose R and S are antisymmetric relations on a set A . Must $R \cup S$ also be antisymmetric? Explain.
11. Let $A = \{a, b\}$, and suppose A has the partial order relation R where $R = \{(a, a), (a, b), (b, b)\}$. Let S be the set of all strings in a 's and b 's and let \leq be the corresponding lexicographic order on S . Indicate which of the following statements are true, and for each true statement cite as a reason part (1), (2), or (3) of the definition of lexicographic order given in Theorem 8.5.1.
- $aab \leq aaba$
 - $bbab \leq bba$
 - $\epsilon \leq aba$
 - $aba \leq abb$
 - $bbab \leq bbaa$
 - $ababa \leq ababaa$
 - $bbaba \leq bbabb$
12. Prove Theorem 8.5.1.
13. Let $A = \{a, b\}$. Describe all partial order relations on A .
14. Let $A = \{a, b, c\}$.
 - Describe all partial order relations on A for which a is a maximal element.
 - Describe all partial order relations on A for which a is a minimal element.
- H 15. Suppose a relation R on a set A is reflexive, symmetric, transitive, and antisymmetric. What can you conclude about R ? Prove your answer.
16. Consider the “divides” relation on each of the following sets A . Draw the Hasse diagram for each relation.
- $A = \{1, 2, 4, 5, 10, 15, 20\}$
 - $A = \{2, 3, 4, 6, 8, 9, 12, 18\}$
17. Consider the “subset” relation on $\mathcal{P}(S)$ for each of the following sets S . Draw the Hasse diagram for each relation.
- $S = \{0, 1\}$
 - $S = \{0, 1, 2\}$

18. Let $S = \{0, 1\}$ and consider the partial order relation R defined on $S \times S$ as follows: For all ordered pairs (a, b) and (c, d) in $S \times S$,

$$(a, b) R (c, d) \Leftrightarrow \text{either } a < c \text{ or both } a = c \text{ and } b \leq d,$$

where $<$ denotes the usual “less than” and \leq denotes the usual “less than or equal to” relation for real numbers. Draw the Hasse diagram for R .

19. Let $S = \{0, 1\}$ and consider the partial order relation R defined on $S \times S$ as follows: For all ordered pairs (a, b) and (c, d) in $S \times S$,

$$(a, b) R (c, d) \Leftrightarrow a \leq c \text{ and } b \leq d,$$

where \leq denotes the usual “less than or equal to” relation for real numbers. Draw the Hasse diagram for R .

20. Let $S = \{0, 1\}$ and consider the partial order relation R defined on $S \times S \times S$ as follows: For all ordered triples (a, b, c) and (d, e, f) in $S \times S \times S$,

$$(a, b, c) R (d, e, f) \Leftrightarrow a \leq d, b \leq e, \text{ and } c \leq f,$$

where \leq denotes the usual “less than or equal to” relation for real numbers. Draw the Hasse diagram for R .

21. Consider the “divides” relation defined on the set $A = \{1, 2, 2^2, 2^3, \dots, 2^n\}$, where n is a nonnegative integer.

- Prove that this relation is a total order relation on A .
- Draw the Hasse diagram for this relation for $n = 4$.

In 22–29, find all greatest, least, maximal, and minimal elements for the relations in each of the referenced exercises.

22. Exercise 16(a) 23. Exercise 16(b)

24. Exercise 17(a) 25. Exercise 17(b)

26. Exercise 18 27. Exercise 19

28. Exercise 20 29. Exercise 21

30. Each of the following sets is partially ordered with respect to the “less than or equal to” relation, \leq , for real numbers. In each case, determine whether the set has a greatest or least element.

- \mathbf{R}
- $\{x \in \mathbf{R} \mid 0 \leq x \leq 1\}$
- $\{x \in \mathbf{R} \mid 0 < x < 1\}$
- $\{x \in \mathbf{Z} \mid 0 < x < 10\}$

31. Let $A = \{a, b, c, d\}$, and let R be the relation

$$R = \{(a, a), (b, b), (c, c), (d, d), (c, a), (a, d), (c, d), (b, c), (b, d), (b, a)\}.$$

Is R a total order on A ? Justify your answer.

32. Let $A = \{a, b, c, d\}$, and let R be the relation

$$R = \{(a, a), (b, b), (c, c), (d, d), (c, b), (a, d), (b, a), (b, d), (c, d), (c, a)\}.$$

Is R a total order on A ? Justify your answer.

33. Consider the set $A = \{12, 24, 48, 3, 9\}$ ordered by the “divides” relation. Is A totally ordered with respect to the relation? Justify your answer.

- H 34. Suppose that R is a partial order relation on a set A and that B is a subset of A . The **restriction of R to B** is defined as follows:

The restriction of R to B

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

In other words, two elements of B are related by the restriction of R to B if, and only if, they are related by R . Prove that the restriction of R to B is a partial order relation on B . (In less formal language, this says that a subset of a partially ordered set is partially ordered.)

35. The set $\mathcal{P}(\{w, x, y, z\})$ is partially ordered with respect to the “subset” relation \subseteq . Find a chain of length 4 in $\mathcal{P}(\{w, x, y, z\})$.

36. The set $A = \{2, 4, 3, 6, 12, 18, 24\}$ is partially ordered with respect to the “divides” relation. Find a chain of length 3 in A .

37. Find a chain of length 2 for the relation defined in exercise 19.

38. Prove that a partially ordered set is totally ordered if, and only if, it is a chain.

39. Suppose that A is a totally ordered set. Use mathematical induction to prove that for any integer $n \geq 1$, every subset of A with n elements has both a least element and a greatest element.

40. Prove that a nonempty finite partially ordered set has

- at least one minimal element,
- at least one maximal element.

41. Prove that a finite partially ordered set has

- at most one greatest element,
- at most one least element.

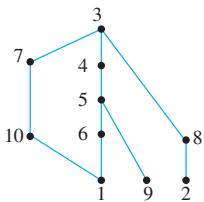
42. Draw a Hasse diagram for a partially ordered set that has two maximal elements and two minimal elements and is such that each element is comparable to exactly two other elements.

43. Draw a Hasse diagram for a partially ordered set that has three maximal elements and three minimal elements and is such that each element is either greater than or less than exactly two other elements.

44. Use the algorithm given in the text to find a topological sorting for the relation of exercise 16(a) that is different from the “less than or equal to” relation \leq .

45. Use the algorithm given in the text to find a topological sorting for the relation of exercise 16(b) that is different from the “less than or equal to” relation \leq .

46. Use the algorithm given in the text to find a topological sorting for the relation of exercise 19.
47. Use the algorithm given in the text to find a topological sorting for the relation of exercise 20.
48. Use the algorithm given in the text to find a topological sorting for the “subset” relation on $\mathcal{P}(\{a, b, c, d\})$.
49. Refer to the prerequisite structure shown in Figure 8.5.1.
 a. Find a list of six noncomparable courses that is different from the list given in the text.
 b. Find two topological sortings that are different from the one given in the text.
50. A set S of jobs can be ordered by writing $x \leq y$ to mean that either $x = y$ or x must be done before y , for all x and y in S . The following is a Hasse diagram for this relation for a particular set S of jobs.



- a. If one person is to perform all the jobs, one after another, find an order in which the jobs can be done.

Task	Time Needed to Perform Task
1	9 hours
2	7 hours
3	4 hours
4	5 hours
5	7 hours
6	3 hours
7	2 hours
8	4 hours
9	6 hours

- a. What is the minimum time required to assemble a car?
 b. Find a critical path for the assembly process.

Answers for Test Yourself

1. for all a and b in A , if $a R b$ and $b R a$ then $a = b$ 2. a and b are any elements of A with $a R b$ and $b R a$; $a = b$ 3. show that there are elements a and b in A such that $a R b$ and $b R a$ and $a \neq b$ 4. all loops; all arrows whose existence is implied by the transitive property; the direction indicators on the arrows 5. $a \leq b$; $b \leq a$ 6. for any two elements a and b in A , either $a \leq b$ or $b \leq a$ 7. a and b are comparable 8. (a) for all b in A either $b \leq a$ or b and a are not comparable (b) for all b in A , $b \leq a$ (c) for all b in A either $a \leq b$ or b and a are not comparable (d) for all b in A , $a \leq' b$ 9. total order; $a \leq' b$ 10. scheduling of tasks