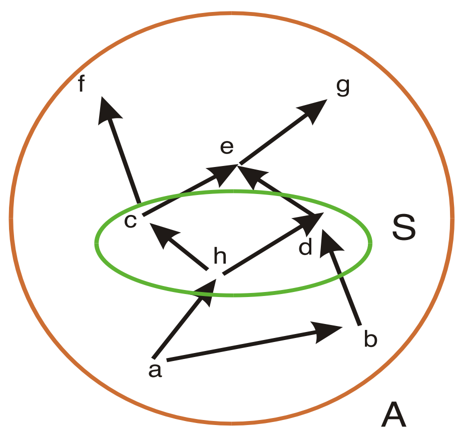
Some notation

- We use symbols like $\sqsubseteq$ to denote partial orderings. This is intended to remind us of specific orderings like $\subseteq$ and $\leq$.
- If $\sqsubseteq$ is a partial ordering on the set A, we put together both A and $\sqsubseteq$ into a pair $(A, \sqsubseteq)$ and call this a poset. The name is a contraction of "partially ordered set."

Maximal and Minimal Elements

- Consider the Hasse diagram below.



S = {c,d,h}; A = {a,b,c,d,e,f,g,h}

- In the set A, there is a *least element* a.
- There is no greatest element in A, but f and g are what we call *maximal elements*.
- We'll look at least and greatest elements, as well as maximal and minimal elements, with respect to subsets of A, like S in the picture.

Formal definitions: various notions of "greatest" and "least"

- **Definition** *Let* $(A, \sqsubseteq)$ *be a poset and* $S \subseteq A$. *An element* $m \in S$ *is the* *greatest* *element of* S *if* $(\forall s \in S)(s \sqsubseteq m)$. *An element* $m \in S$ *is the* *least* *element of* S *if* $(\forall s \in S)(m \sqsubseteq s)$.

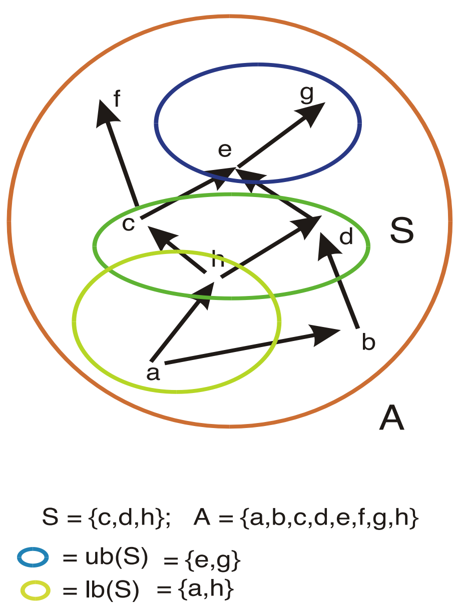
- In the example, a is the least element of A and h is the least element of S. S has no greatest element, and neither does A.

- **Definition** *An element* $m \in S$ *is a* *maximal* *element of* S *if there is no other element* $s \in S$ *with* $m \sqsubseteq s$. *An element* $m \in S$ *is a* *minimal* *element of* S *if there is no other element* $s \in S$ *with* $s \sqsubseteq m$.

- In the example, f and g are maximal elements of A, and c and d are maximal elements of S.

Upper and Lower Bounds

- Given a poset $(A, \sqsubseteq)$ and a subset S of A, we want to look at the elements of A which are "above" and "below" all elements of S.
- **Definition** *We define the set $ub(S)$ of upper bounds of S as $\{x \in A \mid (\forall s \in S)(s \sqsubseteq x)\}$. The set $lb(S)$ of lower bounds of S is $\{x \in A \mid (\forall s \in S)(x \sqsubseteq s)\}$.*
- In the picture, $ub(S)$ and $lb(S)$ are shown.



Least Upper and Greatest Lower Bounds

- **Definition** *If the subset $ub(S)$ has itself a least element, this is called the least upper bound of S. Furthermore, if the set $lb(S)$ has a greatest element, this is called the greatest lower bound of S.*

- In the picture, S has a least upper bound e and a greatest lower bound h. Note that $e \notin S$.

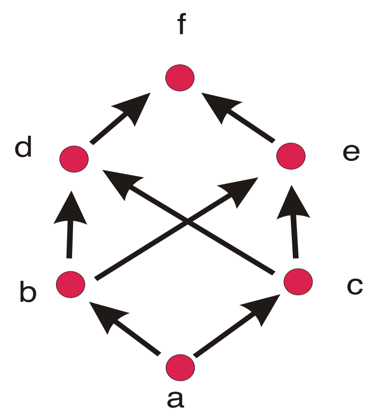
- A subset may fail to have a least upper bound or greatest lower bound. For example, $\{f, g\}$ has a greatest lower bound c but no least upper bound.

- We'll be interested in posets where all two-element subsets have a least upper bound and a greatest lower bound. These are called lattices.

Lattices

- **Definition** *A poset $(A, \sqsubseteq)$ is called a lattice if any two element subset $\{x, y\}$ of A has a least upper bound and a greatest lower bound. These are denoted $x \sqcup y$ and $x \sqcap y$ respectively.*
- Our previous example is not a lattice because $\{f, g\}$ has no least upper bound. But if we remove the element f and the arrow to it, then we do get a lattice.
- Other examples:
    1. $(\mathcal{P}(Z), \subseteq)$. Here the least upper bound of X and Y is $X \cup Y$ annd the greatest lower bound is $X \cap Y$.
    2. The set of divisors of 30 with the divisibility ordering $|$ is a lattice, where $x \sqcup y$ is the least common multiple of x and y, and $x \sqcap y$ is the greatest common divisor of x and y.
    3. The set $\mathbb{N}^+$ of all positive integers is likewise a lattice under the divisibility ordering.

A non-lattice



This is not a lattice, because the set $\{b, c\}$ has no least upper bound. (It does have two minimal upper bounds d and e.)

The divisibility lattice $(\mathbb{N}^+, |)$

- Finding the greatest common divisor and least common multiple of two integers can be done by factoring each number into primes.
- Example:

$$12 = 2^2 \cdot 3 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 \dots$$

$$45 = 3^2 \cdot 5 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^0 \dots$$

- We get the greatest common divisor (gcd) by choosing the minimum exponents:

$$2^0 \cdot 3^1 \cdot 5^0 \cdots = 3$$

- We get the least common multiple (lcm) by choosing the maximum exponents:

$$2^2 \cdot 3^2 \cdot 5^1 \cdot 7^0 \cdots = 180.$$

Unique Factorization

- **Theorem (Fundamental Theorem of Arithmetic.)** *Every positive integer m has a unique factorization into primes of the form*

$$m = p_1^{j_1} \cdot p_2^{j_2} \ldots$$

  where $p_1 = 2, p_2 = 3, \ldots$ are the prime numbers in order, and j_i is the number of times the prime p_i divides m.

  (We called j_i the p_i-level of m in an earlier exercise.)

- Example: $45 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^0 \cdot 11^0 \ldots$.

- This gives rise to a function

$$f(m, i) = p_i\text{-level of } m.$$

- Example: $f(45, 1) = 0; f(45, 2) = 2; f(45, 3) = 1$, and $f(45, i) = 0$ for all $i \geq 4$.

General perspective on gcd and lcm

- **Proposition**

$$m \mid n \iff (\forall i)(f(m,i) \le f(n,i)).$$

- From this, it follows that

$$f(lcm(m,n),i) = \max\{f(m,i), f(n,i)\}$$

and

$$f(gcd(m,n),i) = \min\{f(m,i), f(n,i)\}.$$

- It also follows that $(\mathbb{N}^+, |)$ is a lattice.

- Even more! Notice that $i+j = \max\{i,j\}+\min\{i,j\}$. Therefore

$$\begin{aligned} f(mn,i) &= f(m,i) + f(n,i) \\ &= \max\{f(m,i), f(n,i)\} + \min\{f(m,i), f(n,i)\} \\ &= f((lcm(m,n),i) + f(gcd(m,n),i) \\ &= f(lcm(m,n) \cdot gcd(m,n)), i) \end{aligned}$$

and so

$$mn = lcm(m,n) \cdot gcd(m,n).$$