

The division order on the positive integers

MATH 420/520

NIU

J. B. Stephen

Introduction

We will develop a naive notion of an ordered set, and strongly structured ordered sets called lattices.

Divisibility and positive integers

Consider what we have proven about division in the integers. We restrict our attention to the positive integers, which we denote \mathbb{Z}^+ . We employ the notation $a|b$ for a *divides* b .

- **The definition:** For $a, b \in \mathbb{Z}^+$, a divides b , denoted $a|b$, if
 - b is a multiple of a , or more carefully,
 - there exists $c \in \mathbb{Z}^+$ such that $b = ac$
- **The really simple properties:**
 - for any $a \in \mathbb{Z}^+$, $a|a$ (any integer divides itself), and
 - if $a|b$ and $b|c$, then $a|c$ (if c is a multiple of b and b is a multiple of a , then c is a multiple of a - thus $a|c$).

These properties should look familiar.

The standard order, \leq , on the integers

Consider the integers under \leq , the *less than or equal to* order.

- **The definition:** For $a, b \in \mathbb{Z}$, $a \leq b$ if
 - $b - a$ is 0 or positive, or
 - there exists $c \in \mathbb{N}$ such that $b = a + c$
- **The really simple properties:**
 - for any $a \in \mathbb{Z}$, $a \leq a$ (any integer is less than or equal to itself), and
 - if $a \leq b$ and $b \leq c$, then $a \leq c$ (if c is less than or equal to b and b is less than or equal to a , then c is less than or equal to a - thus $a \leq c$).

Both notions are examples of **ordered sets**.

Relations on sets

We often use symbols to denote certain relationships among elements of a set: exact equality, of numbers, sets, etc., $=$; less than [or equal to] for real numbers, $<$ [\leq]; subset relationships, \subseteq , etc. The symbol $|$ is used to denote the relations *divides* for \mathbb{Z}^+ .

These are all examples of relations on particular sets. Let S be a set, and let \sim be a relation on the set S (so for any two $s, t \in S$, $s \sim t$ if they are related, but they don't have to be related). The symbol \sim is sometimes called, and read as, *tilde*, or when we encounter $r \sim t$ we could just say *r is related to s*.

There are various properties that many relations have in common. For the relation \sim on S

R: if $s \sim s$ for all $s \in S$, then \sim is **reflexive**

* the relations $=$, \leq , \subseteq , and $|$ (divides) discussed above are all reflexive.

S: if whenever $s \sim t$ then $t \sim s$ too, then \sim is **symmetric**.

- * the relation of exact equality $=$ is symmetric, none of the relations \leq , \subseteq , and $|$ (divides) discussed above are symmetric.

T: if whenever $s \sim t$ and $t \sim u$, then $s \sim u$ too, then \sim is **transitive**.

- * the relations $=$, \leq , \subseteq , and $|$ (divides) discussed above are all transitive.

A: if whenever $s \sim t$ and $t \sim s$, then $s = t$, then \sim is **antisymmetric**.

- * the relations $=$, \leq , \subseteq , and $|$ (divides) discussed above are all antisymmetric.
- * Note that if we consider the *divides* relation on \mathbb{Z} , instead of \mathbb{Z}^+ , then it is not antisymmetric. For instance, $2|-2$ and $-2|2$, but $2 \neq -2$.
- * Not all interesting relations are antisymmetric. We commonly divide the integers into the *odds* and the *evens*. This is a relation: $n \sim m$ if they are both even or they are both odd.

A practical example of the antisymmetric nature of *evens* and *odds*.

You leave a room and the desk lamp is on. You come back and the light is turned off. You don't really know exactly how many times the light has been turned on and off, but it has been an odd number of times. Alternatively, if you return and the light is still on you might assume that it has been on all the time you were gone, but it could have been switched any even number of times. So $7 \sim 11$ (both odd - both leave the light off), and $11 \sim 7$, but $7 \neq 11$.

So the even/odd relation is not antisymmetric.

A relation with the properties **R, S, T** (reflexive, symmetric and transitive) is called an **equivalence relation**. We will study these later, and we will also provide a more formal development of relations in general.

A relation with the properties **R, A, T** (reflexive, antisymmetric, transitive) is called an **order relation**.

Order relations

An order relation on a set S is a relation that is reflexive, antisymmetric and transitive (**R, A, T**). We'll use the symbol \preceq to denote an arbitrary partial order, but we pause to consider some examples.

1. Any subset of \mathbb{R} (the reals) with the standard order relation \leq is an ordered set.
2. Any collection \mathcal{U} of sets is ordered under the relation \subseteq .
3. Any subset of \mathbb{Z}^+ is ordered by $a \preceq b$ iff $a|b$.

In the introduction we discussed the features of division that establish that it is an order relation on \mathbb{Z}^+ .

Result 1 $(\mathbb{Z}^+, |)$ is an ordered set. We call the order $a \preceq_d b$ iff $a|b$ the **division order on \mathbb{Z}^+** .

Notice that there are some differences.

For any two real numbers a and b , either $a \leq b$ or $b \leq a$.

An ordered set (S, \preceq) with the property that for all $r, s \in S$ either $r \preceq s$ or $s \preceq r$ is sometimes called a **totally ordered set** or a **linear order**.

For a set S , the power set of S , $\mathcal{P}(S)$ is ordered by \subseteq , but it is not a total order - two subsets of S may not be subsets of one another.

Similarly, given two positive integers a and b , they may not be related by division. For instance, 6 doesn't divide 13 and 13 doesn't divide 6.

If an order relation is not a total order, we say that it is a **partial order**.

Maximums, minimums, meets and joins

For the totally ordered set (\mathbb{R}, \leq) , given any two elements a and b one of them is *bigger* and one of them is *smaller* - we call these the **maximum** and **minimum**, respectively. (They are equal if $a = b$.) So, if $a, b \in \mathbb{R}$, $a \leq b$, then

- $b = \max\{a, b\}$ and
 - $a, b \leq b$, (b is greater than both a and b), and
 - if $a, b \leq c$, then $b \leq c$.
- $a = \min\{a, b\}$ and
 - $a \leq a, b$, (a is less than both a and b), and
 - if $c \leq a, b$, then $b \leq a$.

Let's examine an example.

Example 1 Let S be a set, and let $\mathcal{P}(S)$ be the collection of all subsets of S (including S and \emptyset). The subset relation \subseteq is a partial order on the collection $\mathcal{P}(S)$ - given two subsets $A, B \subseteq S$, it is certainly possible that neither is contained in the other, that is, they are incomparable. Now consider the properties of the sets $A \cup B$ and $A \cap B$:

If $A, B \subseteq S$, then

- $A \cap B \subseteq A, B$, ($A \cap B$ is less than both A and B), and
 - if $C \subseteq A$ and $C \subseteq B$ then $C \subseteq A \cap B$
- $A, B \subseteq A \cup B$, ($A \cup B$ is greater than both A and B), and
 - if $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.

Let's formalize the similarities that we see and make some observations about the division order on \mathbb{Z}^+ .

Definition 1 Let (S, \preceq) be a partially ordered set, and let $a, b, c, d \in S$.

- c is called an lower [upper] bound for a and b if $c \preceq a, b$ [$a, b \preceq c$];
- c is called the **meet** of a and b if
 - c is a lower bound for a and b , $c \preceq a, b$, and
 - if d is any other lower bound for a and b , $d \preceq a, b$, then $d \preceq c$;
- c is called the **join** of a and b if
 - c is an upper bound for a and b , $a, b \preceq c$, and
 - if d is any other upper bound for a and b , $a, b \preceq d$, then $c \preceq d$.

By now we should realize that the partially ordered sets (\mathbb{Z}, \leq) and $(\mathcal{P}(S), \subseteq)$ have the property that each pair of elements has a join and a meet - given by max/min for \mathbb{Z} , and union/intersection for $\mathcal{P}(S)$.

Definition 2 A partially ordered set (S, \preceq) is a **lattice** if every pair of elements of S has both a meet and a join.

You should understand the techniques of proof necessary to establish the following, and the basics covered in this note. These exercise are not assigned for formal write-ups, but an appreciation of the discussed concepts will be assumed from know on. **Exercises:**

1. Verify that $(\mathbb{Z}^+, |)$ is a partially ordered set, and more specifically a lattice. Here $a|b$ is interpreted as an ordering by $a \preceq b \Leftrightarrow a|b$. This is called the **division order on \mathbb{Z}^+** .
2. Explain why the gcd (greatest common divisor) and the LCM (least common multiple) correspond to the meet and join, respectively, in $(\mathbb{Z}^+, |)$.
3. For a particular integer $n \in \mathbb{Z}^+$, let $(S, |)$ be the partially ordered set of all divisors of n . Show that $(S, |)$ is a lattice. [Hint: it suffices to show that if $a, b|n$, then $(a, b)|n$ and $[a, b]|n$. WHY?]
4. (For 420H/520 and extension) Let (S_1, \preceq_1) and (S_2, \preceq_2) be partially ordered sets. A homomorphism of ordered sets is a map $\phi : S_1 \rightarrow S_2$ with the property that for all $p, q \in S_1$, $\phi(p) \preceq_2 \phi(q)$ whenever $p \preceq_1 q$.
 - (a) Show that the map $(\mathbb{Z}^+, |)$ to (\mathbb{Z}^+, \leq) given by $\phi(n) = n$ is a one-to-one homomorphism of ordered sets. Explain why this proves that the gcd (as defined) is the numerically largest common divisor of two positive integers.
 - (b) For a finite set S , show that the map (S, \subseteq) to (\mathbb{N}, \leq) , given by $\phi(A) = |A|$ (number of elements in A) is an order homomorphism, and give an elementary example showing that it is not necessarily one-to-one.