Problems and Comments For Section 4

Problems: 4.4, 4.9, 4.10, 4.15, 4.17,

Comments: For integers m and n we define that m *divides* n, written $m|n$, in case that there is some k such that $k \cdot m = n$. We have,

1. $1|n; n|0$.
2. $n|m$ and $m|n$ if and only if $n = \pm m$.
3. If $a|b$ and $a|c$ then $a|(b+c)$

Instead of saying that a divides b we also say that b *is a multiple of* a.

The *greatest common divisor* (g.c.d.) $d = (m, n)$ of m and n is defined by

1. $d|m$ and $d|n$.
2. If $e|m$ and $e|n$ the $e|d$.

The g.c.d. is unique up to its sign. After you have read section 4, you should be able to prove the following

Proposition *The g.c.d d of m and n is the only common divisor of m and n which is of the form $d = am + bn$.*

The *lowest common multiple* (l.c.m.) $u = [m, n]$ of m and n is defined by

1. $m|u$ and $n|u$.
2. If $m|v$ and $n|v$ then $u|v$.

The l.c.m. is unique up to its sign.

A *partial order* $\leq$ on a set P is a *reflexive, anti-symmetric and transitive* relation. That is, for all $a, b, c \in P$ we have that:

1. $a \leq a$.
2. If $a \leq b$ and $b \leq a$ then $a = b$.
3. If $a \leq b$ and $b \leq c$ then $a \leq c$.
   $(P, \leq)$ is called a *poset*, or *partially ordered* set. A poset is called a *totally ordered* set, or a *chain*, if in addition we have
4. $a \leq b$ or $b \leq a$.

Divisibility restricted to the non-negative integers is a partial order. All real numbers form with respect to ordinary ordering a chain.

An element $u \in P$ is called an *upper bound* of the subset S of P if $u \geq s$ holds for all $s \in S$. An upper bound for S that belongs to S is called the *maximum* of S. Prove that a set S can have at most one maximum. *Lower bounds* and *minima* are similarly defined.

A subset S of the poset P is *bounded above* if it admits an upper bound. A bounded subset is one that admits an upper as well as a lower bound. For the open interval $(0, 1)$ of the totally ordered set $(\mathbb{R}, \leq)$ of real numbers, every number $r \geq 1$ is an upper bound and 1 is the *least upper bound*. Similarly, 0 is the *largest lower bound* for $(0,1)$.

If we restrict divisibility to non-negative integers, then any common divisor of a and b is a lower bound of S and the greatest common divisor is the largest lower bound. Similarly, any common multiple of a and b is an upper bound for S and the lowest common multiple is the least upper bound.

The least upper bound of a subset S of P is called the *supremum* or *join* of S :

$$\sup(S) = \bigvee\{s|\ s \in S\}$$

The largest lower bound of a subset S of P is called the *infimum* or *meet* of S :

$$\inf(S) = \bigwedge\{s|\ s \in S\}$$

A partially ordered set $(L,\leq)$ is called a *lattice* if every two-element subset $S = \{a,b\}$ of L has a join, denoted as $a \vee b$ and meet, denoted as $a \wedge b$. We have that the set $(\mathbb{N}^{+},|)$ of non-negative numbers together with divisibility is a lattice; 0 is the maximum of this lattice where 1 is the minimum. (This is the only case where $a|b$ but $a > b$)

A *complete lattice* is a bounded partially ordered set where every non-empty subset has an infimum as well as a supremum. The power set of a set X is a complete lattice under set inclusion $\subseteq$: For any system $\mathbf{S}$ of subsets of X the join is the union of the sets in $\mathbf{S}$ while the meet is the intersection:

$$\bigvee \mathbf{S} = \bigcup \mathbf{S},\ \bigwedge \mathbf{S} = \bigcap \mathbf{S}$$

If $\mathbf{S} = \{A,B\}$ then the intersection $D = A \cap B$ of $\mathbf{S} = \{A,B\}$ is the largest subset of X, which is contained in A and B. Similarly, the union $U = A \cup B$ is the smallest subset of X which contains A and B.

In a complete lattice L, the infimum of $\mathbf{S} = \emptyset$ is defined as the maximum of L while the supremum of $\mathbf{S} = \emptyset$ is defined as the minimum of L. With this convention in mind, we can drop boundedness in the definition of a complete lattice. In particular, for the powerset lattice $(\mathbf{P}(X),\subseteq)$ of a set X, we define:

$$\bigvee \emptyset = \emptyset,\ \bigwedge \emptyset = X$$

The following is not very difficult to prove:

Theorem *A bounded poset $(P,\leq)$ is already a complete lattice if every subset has an infimum.*