Math 445, Fall 2009 Exercise Set #1 Solutions

1. [#10, page 9] Call a subset B of a set A *cofinite* if the complement of B in A is finite. If B and C are cofinite subsets of A, prove that $B \cap C$ is cofinite.

Proof. We are given that $(A - B)$ and $(A - C)$ are both finite sets. Then by de Morgan's Laws,

$$A - (B \cap C) = (A - B) \cup (A - C)$$

As the union of finite sets is finite, $A - (B \cap C)$ is finite, hence $B \cap C$ is cofinite. □

2. [#2(*), page 13] Let L be a partially ordered set in which *every* subset has a top and bottom element. Prove that L is a finite chain.

Proof. Suppose that L is not finite, then there exists a countably infinite subset of distinct points $X_0 = \{x_k \mid k = 1, 2, \ldots\} \subset L$. We will use induction to construct an infinite subset B_∞ with no top element, which is a contradiction. Hence, L cannot be infinite.

By assumption, there exists both a top and a bottom element for X_0. Let $a_1 = x_{k_1} \in X_0$ denote the top element, and $b_1 = x_{\ell_1} \in X_0$ denote the bottom element of X_0. Set $S_1 = \{a_1, b_1\}$. Note that $b_1 < a_1$ and that the complement $X_1 = X_0 - S_1$ is again infinite.

Now assume that we have chosen a subset $S_n = \{a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n\} \subset X_0$ where each $a_i = x_{k_i} \in X_0$ and $b_i = x_{\ell_i} \in X_0$ are distinct elements, and they satisfy the order relation

$$b_1 < b_2 < \cdots b_n < a_n < \cdots < a_1$$

Set $X_n = X_0 - S_n$. Since X_0 is infinite, the set X_n is again infinite.

By assumption, there exists a top and a bottom element for X_n. Let $a_{n+1} = x_{k_{n+1}} \in X_n$ denote the top element, and $b_{n+1} = x_{k_{m+1}} \in X_n$ denote the bottom element of X_n. Then $b_{n+1} < a_{n+1}$.

Since a_n is the top element of X_n and $a_{n+1} \in X_n - \{a_n, b_n\}$ so $a_{n+1} \neq a_n$ we have that $a_{n+1} < a_n$.

Since b_n is the bottom element of X_n and $b_{n+1} \in X_n - \{a_n, b_n\}$ we have that $b_n < b_{n+1}$.

Then let $S_{n+1} = S_n \cup \{a_{n+1}, b_{n+1}\}$. We are given that $a_{n+1} < a_n$ and $a_n < \cdots < a_1$ hence $a_{n+1} < \cdots < a_1$. Likewise, we are given that $b_n < b_{n+1}$ and $b_1 < \cdots b_n$ so $b_1 < \cdots b_{n+1}$. Combining these inequalities we obtain

$$b_1 < \cdots < b_n < b_{n+1} < a_{n+1} < a_n < \cdots < a_1$$

Set $X_{n+1} = X_0 - S_{n+1}$. Since X_0 is infinite, the set X_{n+1} is again infinite.

Now let $B_\infty = \{b_n \mid n = 1, 2, \ldots\}$. Since the elements are increasing, there can be no top element. □

3. [#3, page 13] Let $\mathbb{N}$ be the chain of positive integers, in its usual order. Is $\mathbb{N}$ complete? Is $\mathbb{N}$ complete if $\omega =$ "∞" is placed on top?

Proof. A set A is *complete* if for every $B \subset A$ there exists a least upper bound $u \in A$ and greatest lower bound $l \in A$. If $A = \mathbb{N}$ then we can let $B = \mathbb{N}$ for example, and while $1 \in \mathbb{N}$ is a greatest lower bound, there is no top element. That is, there is no integer upper bound for the set of integers.

Let $A = \mathbb{N} \cup \{\infty\}$, with the order relation $n < m$ for $n, m \in \mathbb{N}$. Define $n < \infty$ for all $n \in \mathbb{N}$. Given any subset $B \subset A$, there always exists a least element in B which is the greatest lower bound for B. If B is finite, then it has a top element, which is the least upper bound. If B is infinite, then $\infty \in A$ is a least upper bound. So A is complete.

4. [#4, page 13] Let $\mathbb{N}$ be the set of positive integers and define "$m \leq n$" to mean that m divides n. Is $\mathbb{N}$ a lattice? Is it complete? If not, how could we make it complete?

Proof. First we show this defines a partial order on $\mathbb{N}$. Clearly, for all $m \in \mathbb{N}$, m divides m so $m \leq m$.

If $m \leq n$ then there exists an integer $p \in \mathbb{N}$ such that $n = p \cdot m$. If $n \leq m$ then there exists an integer $q \in \mathbb{N}$ such that $m = q \cdot n$. Thus, $n = p \cdot m = p \cdot q \cdot n$ which implies that $1 = p \cdot q$. As both p, q are positive integers, this implies $p = q = 1$ and hence $m = n$.

Let $m \leq n$ and $n \leq t$. Then there exists integers $p, q \in \mathbb{N}$ such that $n = p \cdot m$ and $t = q \cdot n$. Thus, $t = p \cdot (q \cdot m) = (pq) \cdot m$ so $m \leq t$. Let $\mathbb{N}_*$ denote the set $\mathbb{N}$ with this partial order.

Next we show that $\mathbb{N}_*$ is a lattice. Given $m, n \in \mathbb{N}_*$ let $\gcd\{m, n\}$ be the least common denominator of $\{m, n\}$ and let $\operatorname{lcm}\{m, n\}$ denote the least common multiple of $\{m, n\}$. These exists due either to some ancient Greek, or to some ancient Chinese mathematicians. Then $\gcd\{m, n\}$ is the greatest lower bound of the set $\{m, n\}$ - essentially by definition. Similarly, $\operatorname{lcm}\{m, n\}$ is the least upper bound of $\{m, n\}$. Thus, $\mathbb{N}_*$ is a lattice for this partial order.

The lattice is not complete. Let $p > 1$ be a prime. Define $C_p = \{a_n = p^n \mid n = 1, 2, \ldots\} \subset \mathbb{N}_*$. Since $a_n \leq a_{n+1}$ for this partial order, there is no upper bound for the chain C_p.

How can we make $\mathbb{N}_*$ complete? First, we must add to $\mathbb{N}_*$ an upper bound for each chain C_p. Let p^∞ denote the upper bound for C_p (This is much like adding ∞ to $\mathbb{N}$ in the previous exercise.)

Next, $m \in \mathbb{N}_*$ with a prime factorization $m = p_1^{\ell_1} \cdots p_k^{\ell_k}$ where each $p_i > 1$ and $\ell_i \geq 1$. If $k > 1$ then no prime power p^m is comparable to m hence we must add a point at infinity m^∞ which is an upper bound for the chain C_m formed by the powers of m.

But this also does not suffice. Can you find a chain for which none of these additional "infinities" is an upper bound? In fact, it is necessary to add an uncountable number of upper bounds, or infinities to $\mathbb{N}_*$ to compactify this set. So we have not even come close yet to finding all the upper bounds we need to add. □

5. [#9, page 13] Let L be a distributive lattice with a top element "1" and a bottom element "0". (Recall this means that $0 \leq a \leq 1$ for all $a \in L$.) Prove that if an element $a \in L$ has a complement, then the complement a' is unique.

Proof. Recall that $b \in L$ is a *complement* for a, if b satisfies $a \cup b = 1$ and $a \cap b = 0$.

Let $b, c \in L$ be complements for a. We will show that $c \leq b$ and $b \leq c$, hence $b = c$. Thus, one can define $a' = b$ or $a' = c$, unambiguously.

First, $a \cup c = 1$ and $b \cap a = 0$ implies

$$b = b \cap 1 = b \cap (a \cup c) = (b \cap a) \cup (b \cup c) = 0 \cup (b \cap c) = b \cup c$$

from which we conclude by the definitions that $c \leq b$. But also, $a \cup b = 1$ and $c \cap a = 0$ implies

$$c = c \cap 1 = c \cap (a \cup b) = (c \cap a) \cup (c \cup b) = 0 \cup (c \cap b) = c \cup b$$

Hence $b \leq c$, as was to be shown. □

6. [#7, page 17] Given a function $f\colon A \to A$, we write f^n for the function on A obtained by taking the composite of f with itself n times. Suppose that f^n equals the identity function for some n (one then says that f is *periodic*.) Prove that such f is one-to-one and onto.

Proof. Suppose that $f^n = id$. Set $g = f^{n-1}$. Then $f \circ g = g \circ f = Id$, so the map f has an inverse g. Therefore, f is one-to-one and onto. ☐

7. [#8, page 17] As a generalization of periodic functions, we say that $f\colon A \to A$ is *locally periodic* if for every $x \in A$ there exists an integer $n(x) \geq 1$, depending on x, such that $f^{n(x)}(x) = x$. Prove that a locally periodic function is one-to-one and onto.

Proof. This problem is like the above, except we cannot just write down the inverse function. We must show that f is one-to-one, and then show it is onto.

We first show that f is 1-1. Let $y, z \in A$ and suppose that $f(y) = f(z)$. Let $m = n(y)$ and $n = n(z)$.

Observe that $y = f^m(y)$, so $y = f^m(f^m(y)) = f^{2m}(y)$ and we can iterate this as many times as needed. In particular, $y = f^{nm}(y)$.

Similarly, $z = f^n(z)$, so $z = f^n(f^n(z)) = f^{2n}(z)$ and we can iterate this as many times as needed. In particular, $z = f^{mn}(z)$.

Thus, $y = f^{nm}(z) = f^{nm-1}(f(z)) = f^{nm-1}(x)$ and $z = f^{mn}(z) = f^{mn-1}(f(z)) = f^{mn-1}(x)$.

So $y = f^{nm-1}(x) = f^{mn-1}(x) = z$.

Next, we show that f is onto, which is simpler. Let $x \in A$, then $x = f^{n(x)}(x) = f(f^{n(x)-1}(x))$. Set $w = f^{n(x)-1}(x) \in A$, then $x = f(w)$. ☐

8. [#14, page 18] Fix a set A. For a subset $S \subset A$, the characteristic function ϕ_S of S is the function from A to the set $\{0, 1\}$ which takes the value 1 on every element of S, and the value 0 on every element of the complement $S' = A - S$. Prove, for subsets $S, T \subset A$:

(1) $\phi_{S\cap T} = \phi_S \cdot \phi_T$ (the product of the two functions)
(2) $\phi_{S'} = 1 - \phi_S$
(3) $\phi_S + \phi_T = \phi_{S\cup T} + \phi_{S\cup T}$ (note typo!)

Proof. Rule (1) is typical:

$$\phi_{S\cap T}(x) = 1 \iff x \in S \cap T \iff x \in S \;\&\; x \in T \iff \phi_S(x) = 1 \;\&\; \phi_T(x) = 1 \iff \phi_S(x) \cdot \phi_T(x) = 1$$

Rules (2) and (3) follow the same pattern. ☐