Exercises 43, 46, 51, 52

Exercise 43

Claim: $\forall a, b \in A, \exists c \in A$ such that $a \wedge b = c$

Proof: The greatest lower bound between $a, b \in A$, i.e. $a \wedge b$, is the greatest common divisor of a and b, $\gcd(a, b)$, because A is ordered by divisibility, the greatest $c \in A$ such that $c \leq a$ and $c \leq b$ is by definition the greatest $c \in A$ such that c divides a and c divides b – the definition of $\gcd(a, b)$. Such a c exists because (not sure if I have to prove this but this is elementary school math) $\gcd(a, b)$ is the product of every element in the intersection of the prime factors of a and of b, which are included in A because A is the set of all the positive integer divisors of n.

Claim: $\forall a, b \in A, \exists c \in A$ such that $a \vee b = c$

Proof: The lowest upper bound between a and b, i.e. $a \vee b$, is the least common multiple of a and b, $\mathrm{lcm}(a, b)$, because A is ordered by divisibility, the smallest $c \in A$ such that $c \geq a$ and $c \geq b$ is by definition the smallest $c \in A$ such that a and b both divide c – the definition of $\mathrm{lcm}(a, b)$. Such a c exists because (again, elementary school math so I hope I don't gotta prove it), $\mathrm{lcm}(a, b)$ is the product of every element in the union of the prime factors of a and b, which are included in A because A is the set of all the positive integer divisors of n.

Claim: n is the one (or unit) of A

Proof: n is the least upper bound of all the elements of A because by definition of A, every element in A divides n, so $\forall c \in A, c \leq n$.

Claim: 1 is the zero of A

Proof: 1 is the greatest lower bound of all the elements of A because 1 divides every positive integer, so it divides everything in A, so $\forall c \in A$, $1 \leq c$.

Claim: $(A, \leq)$ is distributive, i.e. $\forall x, y, z \in A$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

Proof: $x \wedge (y \vee z) = \gcd\big(x, \mathrm{lcm}(y, z)\big)$. Let X be the set of all prime factors of x (we know we aren't "losing" any due to repetition because it is given that n has no square factors $f > 1$). Let Y be the set of all prime factors of y. Let Z be the set of all prime factors of z. $\gcd\big(x, \mathrm{lcm}(y, z)\big) = X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z) = \mathrm{lcm}(\gcd(x, y), \gcd(x, y)) =$ $(x \wedge y) \vee (x \wedge z)$.

Claim: if $\forall a \in A, \neg a = n \div a$, then $a \vee \neg a = one = n$ and $a \wedge \neg a = zero = 1$

Proof: $a \vee \neg a = \mathrm{lcm}(a, \neg a) = n$, because firstly, n divides both a and $\frac{n}{a}$, and secondly, a and $\frac{n}{a}$ don't share any prime factors (i.e. the intersection between their prime factors is the empty set) because of the fact that n doesn't have any square factors $f > 1$; so, if X is the set of all of a's prime factors, then $\frac{n}{a}$ is the product of all elements of the set $P \setminus X$, where P is the set of all of n's prime factors. Thus, the least common multiple must be their product: $a \times \frac{n}{a} = n$.

$a \wedge \neg a = \gcd(a, \neg a) = 1$ because as we said in the previous paragraph, a and $\frac{n}{a}$ don't share any prime factors.

Claim: the prime divisors of n are the atoms of $(A, \leq)$.
Proof: For each prime divisor p of n, there's no smaller non-zero element because any element $s \in A$ such that $s < p$ means $s \neq p$ and s divides p, and because of the definition of prime, whose only positive divisors are 1 and p, s has to be 1, which is the zero of A.

Claim: the theorem given earlier in the notes is the unique factorization theorem for n.
Proof: The theorem given earlier is, "in a finite Boolean algebra, each element is the lub of a (unique) finite set of atoms". $(A, \leq)$ is finite. n is the product of all of its prime factors, i.e. if we define S to be the set of all atoms of $(A, \leq)$ (i.e. all prime factors of n), then $n = \prod_{s \in S} s$. This is equal to $\text{lcm}_{s \in S}\, s$, or $\bigvee_{s \in S} s$.

Exercise 46

Claim: the Boolean algebra of finite unions of left closed right open intervals in the rationals is atomless
Proof: We already proved this in the last homework, in Exercise 40 part b.

Claim: the Boolean algebra of finite unions of left closed right open intervals in the rationals is not complete
Proof: The least upper bound of all left closed right open intervals $[n, n+1[$ where $\exists k \in \mathbb{N}$ such that $n = 2k$ (i.e. left closed right open intervals that start at an even number and are of length one) does not exist because that would be the union of all of them, but there are an infinite number of them, so it would be an infinite union, but the set we're dealing with only has finite unions.

Exercise 51

a) There's at least one element in A between v_0 and v_1, and v_0 is less than v_1
b) v_0 is not strictly less than v_1
c) There's at least one element v_2 in A such that v_0 is strictly less than v_1 and that v_2 is greater than v_1. Though, if v_0 is less than v_1 for one element in A, then it's true

in all instances, because the statement $v_0 < v_1$ has nothing to do with v_2. So, the statement can be reduced to $\boxed{v_0 \text{ is less than } v_1 \text{ and there's at least one element in } A \text{ greater than } v_1}$.

d) :

a. There's at least one non-negative integer between the two non-negative integers v_0 and v_1, where $v_0 < v_1$

b. The non-negative integer v_0 is not strictly less than the non-negative integer v_1

c. The non-negative integer v_0 is less than the non-negative integer v_1 and at least one non-negative integer is greater than v_1, but every non-negative integer is less than some other non-negative integer, so, this statement can be reduced to $\boxed{\text{the non-negative integer } v_0 \text{ is less than the non-negative integer } v_1}$

e) :

a. There's at least one subset $S \subseteq \{a, b, c\}$ such that it properly includes subset v_0 and is properly included by subset v_1

b. Subset v_0 is not properly included by subset v_1

c. Subset v_0 is properly included by subset v_1, and there's at least one subset $S \subseteq \{a, b, c\}$ such that it properly includes v_1

f) :

a. there's at least one positive divisor of 30 that's not v_0 or v_1 (who are also positive divisors of 30), and it is divisible by v_0 and is a divisor of v_1

b. v_0 is not a divisor of v_1, and both are positive divisors of 30

c. v_0 does not equal v_1, and v_0 is a divisor of v_1, and there's at least one positive divisor of 30 that's not v_0 or v_1 such that it is divisible by v_1

Exercise 52

a) Assume $(\forall v_i)\big(\phi(v_i)\big)$, want to prove $\neg(\exists v_i)\big(\neg\phi(v_i)\big)$.
Consider an arbitrary sequence $x \in A^\omega$, then x satisfies $(\forall v_i)\big(\phi(v_i)\big)$ by assumption. Since it satisfies it, it also means we can choose a sequence $y \in A^\omega$ such that $(\forall j \neq i)\big(y_j = x_j\big)$ and y satisfies $\phi(v_i)$ for all v_i (clauses 6 and 1). For $\neg(\exists v_i)\big(\neg\phi(v_i)\big)$ to be true, x has to not satisfy $(\exists v_i)\big(\neg\phi(v_i)\big)$, that is, iff there's no sequence $z \in A^\omega$ such that $(\forall j \neq i)\big(z_j = x_j\big)$ and z does not satisfy $\phi(v_i)$ for some v_i, which is valid because we just proved that for all sequences z such that $(\forall j \neq i)\big(z_j = x_j\big)$, z satisfies $\phi(v_i)$ for every v_i!

Assume $\neg(\exists v_i)\big(\neg\phi(v_i)\big)$, want to prove $(\forall v_i)\big(\phi(v_i)\big)$.

Consider an arbitrary sequence $x \in A^\omega$, then x satisfies $\neg(\exists v_i)\big(\neg\phi(v_i)\big)$ by assumption. Since it satisfies it, it means x does not satisfy $(\exists v_i)\big(\neg\phi(v_i)\big)$. So, there does not exist a sequence $y \in A^\omega$ such that $(\forall j \neq i)\big(y_j = x_j\big)$ and y does not satisfy $\phi(v_i)$ for some v_i. This means for all sequences y such that $(\forall j \neq i)\big(y_j = x_j\big)$, y satisfies $\phi(v_i)$ for all v_i, which is $(\forall v_i)\big(\ \phi(v_i)\big)$!

b) Assume $(\exists v_i)\big(\phi(v_i)\big)$, want to prove $\neg(\forall v_i)\big(\neg\phi(v_i)\big)$.
Consider an arbitrary sequence x, then x satisfies $(\exists v_i)\big(\phi(v_i)\big)$ by assumption. Since it satisfies it, it means we can choose a sequence y such that $(\forall j \neq i)\big(y_j = x_j\big)$ and y satisfies $\phi(v_i)$ for some v_i. The existence of such a sequence y means there's no sequence z such that $(\forall j \neq i)\big(z_j = x_j\big)$ and that z does not satisfy $\phi(v_i)$ for every v_i, which is $\neg(\forall v_i)\big(\neg\phi(v_i)\big)$.

Assume $\neg(\forall v_i)\big(\neg\phi(v_i)\big)$, want to prove $(\exists v_i)\big(\phi(v_i)\big)$.
Consider an arbitrary sequence x, then x satisfies $\neg(\forall v_i)\big(\neg\phi(v_i)\big)$ by assumption. Since it satisfies it, it means x does not satisfy $(\forall v_i)\big(\neg\phi(v_i)\big)$, which means there's no sequence y such that $(\forall j \neq i)\big(y_j = x_j\big)$ and y does not satisfy $\phi(v_i)$ for all v_i. This means there's some sequence z such that $(\forall j \neq i)\big(z_j = x_j\big)$ and z satisfies $\phi(v_i)$ for some v_i, which is $(\exists v_i)\big(\phi(v_i)\big)$.