Logics

FAMAF - UNC

SLP

Contents

1 Functions

A FUNCTION $f : A \mapsto B$ is a set of tuples $\{(a,b) : a \in A \text{ and } b \in B\}$. The domain $\mathcal{D}_f$ and image I_f of a function have the usual definitions. The kernel of a function is

$$ker(f) = \left\{(a,b) \in \mathcal{D}_f^2 : f(a) = f(b)\right\}$$

From this follows that a function f is injective—that it maps to each element in $\mathcal{D}_f$ a distinct element in the range—iff $ker(f) = \left\{(a,b) \in \mathcal{D}_f^2 : a = b\right\}$.

Given $F : A \mapsto B$ and $S \subseteq A$, we will use $F(S)$ to denote $\{F(a) : a \in S\}$.

2 Equivalence relations

EQUIVALENCE RELATIONS are a formalization of the notion that certain elements in a set are in some sense equivalent. This sense might be functional (e.g. they map to identical values via some function F) or structural (e.g. the elements are in the same level of a Hasse diagram).

Definition 1. Given a set A, a binary relation over A is a subset of A^2.

Observe that $\emptyset$ is a binary relationship over any set A. We use $A \propto B$ to say "A is a binary relation over B". The notation aRb is a shorthand for $(a, b) \in R$.

Observe that $R \propto A$ and $A \subseteq B$ implies $R \propto B$. Many properties of the $\propto$ relation follow from the properties of the $\subseteq$ relation. The properties that a binary relation R *may* follow are the following, given any $R \propto A$:

- $\propto$ is reflexive: aRa for any $a \in A$.
- $\propto$ is transitive: aRb and bRc implies aRc for any $a, b, c \in A$.
- $\propto$ is symmetric: $aRb \Rightarrow bRa$ for any $a, b \in A$.
- $\propto$ is anti-symmetric: aRb and bRa implies $a = b$ for any $a, b \in A$.

Whether and which of these properties hold depends on the sets in question.

Example. Consider $R = \left\{(x, y) \in \mathbb{N}^2 : x \leq y\right\}$. Then $R \propto \mathbb{N}$ and $R \propto \omega$. However, R is reflexive with respect to $\mathbb{N}$ but not with respect to ω, because $(0, 0) \notin R$.

Definition 2. An equivalence relation over A is a binary relation $R \propto A$ s.t. R is reflexive, transitive and symmetric with respect to A.

We write $R \ddot{\propto} A$ to say R is an equivalence relation over A.

Problem 1. Determine true or false for the following statements.

(1) Given X a set, then $R = \emptyset$ is a binary relation over X that is transitive, symmetric and anti-symmetric with respect to X.

We know $\emptyset \propto X$ for any X. Recall that xRx is a shorthand for $(x, x) \in R$ where R is a binary relation. In particular, $(x, x) \notin \emptyset$ for any $x \in X$, so $\emptyset$ is not reflexive. The same applies to all other properties. The statement is false.

(2) If $R \propto X$ and R is not anti-symmetric with respect to X, then R is symmetric with respect to X.

The statement is false. Consider $R = \{(1, 2), (2, 1), (5, 3)\}$ where $R \propto \omega$. Evidently R is not anti-symmetric over ω, because $1R2$ and $2R1$ and yet $2 \neq 1$. However, it is also not symmetric, because $5R3$ and $\neg(3R5)$.

(3) If A a set then $A^2 \propto A$.

Trivially true, since $A^2 \subseteq A^2$.

(4) If $R = \{(x, y) \in \mathbb{N}^2 : x = y\}$ *then* $R \ddot{\propto} \omega$.

By definition xRx holds. Evidently, $xRy \Rightarrow yRx$ so it is symmetric. Furthermore, $xRy \wedge yRz \Rightarrow xRz$. The statement is true.

(5) If $R \ddot{\propto} B$ and $A \subseteq B$ then $R \ddot{\propto} A$.

We need not even impose the constraint of an *equivalence* relation since the statement is false for any binary relation. In fact, $R \subseteq B^2$ and $A \subseteq B$ does not imply $R \subseteq A^2$. For example, $R = \{(1, 2), (2, 3), (3, 4)\} \subseteq \omega^2$ and $A = \{1, 2\} \subseteq \omega$. However, $R \not\ddot{\propto} A$. Since the statement is false for all binary relations, and equivalence relations are a form of binary relation, the statement is false.

Definition 3. The equivalence class of $a \in A$ with respect to equivalence relation $R \ddot{\propto} A$ is

$$[a]_R = \{b \in A : aRb\}$$

.

We sometimes write simply $[a]$ if the equivalence relation R is understood by the context. We may also write a/R to denote the equivalence class $[a]_R$.

Example. Let $R = \{(x, y) \in \mathbb{Z}^2 : x \text{ has the same parity than } y\}$. Then $[2]$ denotes the set of all numbers that have the same parity than 2; this is, all even numbers.

If $R = \{(x, y) \in \mathbb{Z}^2 : 5 \mid x - y\}$ then $[0] = \{5t : t \in \mathbb{Z}\}$.

Problem 2. If $R \ddot{\propto} A$ and $a \in A$ then $a \in [a]$.

True because R is reflexive: $aRa \Rightarrow a \in [a]$ by definition.

Problem 3. If $R \ddot{\propto} A$ and $a, b \in A$, then $aRb \iff [a] = [b]$.

Assume aRb. Then, for any $x \in [b]$, transitivity tells us aRx. And because $aRb \Rightarrow bRa$ we have, via the same argument, that for any $y \in [a]$ bRy. Of course,

$$\langle \forall x : x \in A : x \in B \rangle \wedge \langle \forall y : y \in B : y \in A \rangle \Rightarrow A = B$$

So $[a] = [b]$. ■

If we assume $[a] = [b]$ then of course $aRx \iff bRx$. By symmetry we have xRa and then by transitivity $bRx \wedge xRa \Rightarrow bRa \Rightarrow aRb$. ■

Problem 4. Let $R \ddot{\propto} A$ and $a, b \in A$. Then $[a] \cap [b] = \emptyset$ or $[a] = [b]$.

Assume $[a] \cap [b] \neq \emptyset$ and $[a] \neq [b]$, which is the negation of the statement we want to prove. Since $[a] \neq [b]$ we cannot have aRb, due to what was proven in the previous exercise. However, since $[a] \cap [b] \neq \emptyset$ there is some $z \in A$ s.t. aRz and bRz. However, $bRz \Rightarrow zRb$ and then aRb by transitivity. This is a contradiction. Then the statement is true.

Definition 4. We use A/R to denote $\{[a] : a \in A\}$ and call this set the quotient of A by R.

In other words, given $R \ddot{\propto} A$, the quotient of A by R is the set of all equivalence classes. For example, if $R = \{(x, y) \in \mathbb{R}^2 : x = y\}$ then $\mathbb{R}/R = \{\{x\} : x \in \mathbb{R}\}$.

Definition 5. If $R \ddot{\propto} A$, we define $\pi_R : A \mapsto A/R$ defined as $\pi_R(a) = a/R$ for every $a \in A$. We call this function the **canonic projection** with respect to R.

Theorem 1. *If $R \ddot{\propto} A$, then $ker(\pi_R) = R$. This entails that π_R is injective iff $R = \left\{(x, y) \in A^2 : x = y\right\}$.*

Proof 1. Recall that $ker(f) = \left\{(a, b) \in \mathcal{D}_f^2 : f(a) = f(b)\right\}$. The canonic projection π_R maps elements of a set to their equivalence class over R. It follows that $\pi_R(a) = \pi_R(b)$ iff $[a] = [b]$. So

$$\begin{aligned} ker(\pi_R) &= \{(a, b) : [a] = [b]\} \\ &= \{(a, b) : aRb\} \\ &= R \blacksquare \end{aligned}$$

Assume π_R is injective. Then no two distinct elements can have the same equivalence class. Which entails no two distinct elements are qeuivalent. $\therefore$ $R = \left\{(a, b) \in A^2 : a = b\right\}$. $\blacksquare$ The other direction of the implication is trivial.

Problem 5. Let $R = \left\{(x, y) \in \mathbb{Z}^2 : 5 \mid x - y\right\}$. Find $\mathbb{Z}/R$.

Observe that $(5, 0), (6, 1), (7, 2), (8, 3), (9, 4) \in R$. From that point onward (and from $(5, 0)$ downward) we deal with the same equivalence class.

More formally, $[5] = \{5t : t \in \mathbb{Z}\}$, $[6] = \{1, 6, 11, \ldots\} = \{5t + 1 : t \in \mathbb{Z}\}$. In general, if $A(k) = \{5t + k : t \in \mathbb{Z}\}$, then

$$\{A(0), A(1), \ldots, A(4)\} = \mathbb{Z}/R$$

Observe that this can be generalized. If $R = \{(x, y) : z \mid x - y\}$ for some fixed $z \in \mathbb{N}$, then

$$\{\{zt : t \in \mathbb{Z}\}, \{zt + 1 : t \in \mathbb{Z}\}, \ldots, \{zt + (z - 1) : t \in \mathbb{Z}\}\} = \mathbb{Z}/R$$

and $|\mathbb{Z}/R| = z$.

Problem 6. Let $R = \left\{(x, y) \in \mathbb{N}^2 : x, y \leq 6\right\} \cup \left\{(x, y) \in \mathbb{N}^2 : x > 6 \land y > 6\right\}$. Prove that R is an equivalence relation over $\mathbb{N}$ and find $\mathbb{Z}/R$. How many elements does it have?

(1) Let $(a, b) \in R$. We have two possible cases. If (a, b) is s.t. $a, b \leq 6$, then if bRc for some $c \in \mathbb{N}$ we must have $c \leq 6$. This implies $(a, c) \in R$, which means the relation is transitive. A similar argument shows transitivity applies to the case $a, b > 6$. It is very simple to show that the relation is reflexive. To show it is symmetric, simply observe that $(a, b) \in R$ implies either $a, b \leq 6$ or $a, b > 6$ which implies $(b, a) \in R$.

(2) Evidently, $6R5, 6R4, 6R3, \ldots$, and $7R8, 7R9, 7R10, \ldots$. Thus, the equivalence relation R over $\mathbb{Z}$ has a quotient space

$$\mathbb{Z}/R = \{\{z \in \mathbb{Z} : z \leq 6\}, \{z \in \mathbb{Z} : z > 6\}\} = \{6/R, 7/R\}$$

Problem 7. Give true or false for the following statements.

(1) If R an equivalence relation over $A \neq \emptyset$, then $|A/R| = 1 \iff R = A \times A$.

> ($\Leftarrow$) It is easy to see that $R = A \times A$ is by definition the equivalence relation where any $a \in A$ is equivalent to any $b \in A$. So $|R/A| = 1$.
>
> ($\Rightarrow$) Let $R = A \times A$. Assume $|A/R| \neq 1$. Since $A \neq \emptyset$, $A \times A \neq \emptyset$ and $|A/R| > 0$. So we must have $|A/R| > 1$. This implies there is some $a, b \in A$ s.t. $\neg(aRb)$ (otherwise a unique equivalence class would exist). But then $(a, b) \notin A^2$, which contradicts the definition of Cartesian product. Then if $R = A \times A$, $|A/R| = 1$.
>
> In conclusion, the statement is true.

(2) If $R \ddot{\propto} A$ then $A/R = \{\{a/R\} : a \in A\}$.

> False. By definition: $A/R = \{a/R : a \in A\} \neq \{\{a/R\} : a \in A\}$

(3) Let $R \ddot{\propto} A$ with $A = \{1, 2, 3, 4, 5\}$. Then $|\,\{i/R : i \in A\}\,| = 5$.

> False. It depends on R, which is unspecified. E.g. we have shown that if $R = A^2$ then $|A/R| = 1$.

(4) $A/\big\{(x, y) \in A^2 : x = y\big\} = A$.

> False, but easy to mistake as true. By definition of $R = \big\{(x, y) \in A^2 : x = y\big\}$ we have $x, y \in A \wedge x \neq y \Rightarrow \neg(xRy)$. So $a \in A$ belongs to a singleton class a/R. Then $A/R = \{\{a\} : a \in A\} \neq A$.

(5) Let $R \ddot{\propto} A$ and $C \subseteq A, C \neq \emptyset$. Assume xRy for any $x, y \in C$. Then $C \in A/R$.

> The statement is false. Observe that
>
> $$c/R = C \cup \{x \in A : x \notin C \wedge cRx\}$$
>
> If the second set is non-empty then $C \notin A/R$.
>
> **Counter example.** Let $A = \{1, 2, 3, 4, 5\}$ and $C = \{1, 2\}$, satisfying the constraints of the problem. If $(1, 3) \in R$ and we assume no non-reflexive relations other than $(1, 2), (1, 3)$ exist, then $A/R = \{\{1, 2, 3\}\} \not\ni C$.

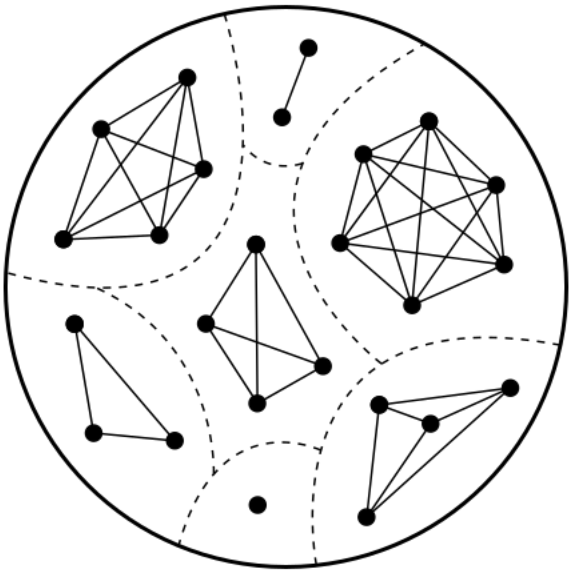
Problem 8. Let $R \ddot{\propto} A$. Prove *(1)* that $ker(\pi_R) = R$ and *(2)* π_R is injective iff $R = \big\{(x, y) \in A^2 : x = y\big\}$.

(1) By definition $\pi_R(a) = a/R$ which entails that $ker\ \pi_R = \{(a, b) : a/R = b/R\}$. Of course $a/R = b/R \iff aRb$. Then $ker(\pi_R) = \{(a, b) : aRb\} = \{(a, b) : (a, b) \in R\} = R$.

(2) ($\Rightarrow$) Assume π_R is injective. Then no two elements in the domain map to the same element. Then $\pi_R(a) \neq \pi_R(b)$ for all $a, b \in A, a \neq b$, which entails $a/R \neq b/R$ for all $a, b \in A, a \neq b$. Then each element is only equivalent to itself. Then $R = \big\{(a, b) \in A^2 : a = b\big\}$.

($\Leftarrow$) Assume $R = \big\{(a, b) \in A^2 : a = b\big\}$. Then $\neg(aRb)$ for any $a, b \in A, a \neq b$. Then $\pi_R(a) \neq \pi_R(b)$ for all $a, b \in A, a \neq b$. Then π_R is injective.

Figure 1: Graph of a quotient space with 7 equivalent classes. Any two connected vertices denote equivalent elements of a set.



2.1 Partitions and equivalence

A PARTITION $\mathcal{P}$ of a set A is a set s.t. every $P \in \mathcal{P}$ is a subset of A, $P_1 \cap P_2 = \emptyset$ for any $P_1, P_2 \in \mathcal{P}, P_1 \neq P_2$; and $\bigcup_{P \in \mathcal{P}} P = A$.

Given a partition $\mathcal{P}$ of a set A, a valid binary relation is

$$R_{\mathcal{P}} = \{(a, b) : a, b \in S \text{ for some } S \in \mathcal{P}\}$$

Observe that $R_{\mathcal{P}}$ is an equivalence relation. First of all, $aR_{\mathcal{P}}a$ because a is always in the same partition than a. Furthermore, if $aR_{\mathcal{P}}b$ and $bR_{\mathcal{P}}c$ then a and c are in the same partition. Lastly, if a is in the same partition than b, then b is in the same partition than a (symmetry).

Furthermore, if $R \ddot{\propto} A$ is an arbitrary equivalence relation, then A/R is a partition of A. To each element $a \in A$ corresponds some a/R that contains *at least* a; from this follows trivially that $\bigcup_{a \in A} a/R = A$. Furthermore, if $a/R \neq b/R$ for some $a, b \in A$, then $a/R \cap b/R = \emptyset$—otherwise, some element $c \in A$ equivalent to a and b should exist, but this would contradict the hypothesis that a and b are not equivalent. That $a/R \subseteq A$ for every $a \in A$ follows trivially from the definition of equivalence class.

Theorem 2. *Let A an arbitrary set, $\mathscr{P}_A$ the set of all partitions of A and $\mathscr{R}_A$ the set of all binary equivalence relations over A. Then*

$$\begin{aligned} \mathscr{P}_A &\mapsto \mathscr{R}_A \\ \mathcal{P} &\mapsto R_{\mathcal{P}} \end{aligned} \qquad\qquad \begin{aligned} \mathscr{R}_A &\mapsto \mathscr{P}_A \\ R &\mapsto A/R \end{aligned}$$

are bijections one the inverse of the other.

Proof 2. Complete.

Problem 9. Say true, false or imprecise the following statements.

(1) If $\mathcal{P}$ a partition of X and $x \in X$, then $x/\mathcal{P} \in \mathcal{P}$.

> Imprecise. $\mathcal{P}$ is a partition, not a binary relation, and thus the expression $x/\mathcal{P}$ is undefined.

(2) $\mathcal{P} = \{1, 3/2, 4/5, 6\}$ is a partition of $\{1, 2, 3, 4, 5, 6\}$.

> Imprecise. The expression $3/2, 4/5$, etc. are undefined.

(3) If $\mathcal{P}$ a partition of X, then $\mathcal{P} \cap X = \emptyset$.

> The statement is true. The set $\mathcal{P}$ contains *sets* of elements of X; the set X contains elements of X. Therefore, each $P \in \mathcal{P}$ is of a different type than each $x \in X$.

(4) If $R \mathrel{\ddot{\propto}} A$, then $A \cap A/R = \emptyset$.

> We know A/R is a partition of A, and in the previous problem we have already stated that $A \cap \mathcal{P} = \emptyset$ for any partition $\mathcal{P}$ of A. So the statement is true.

(5) If $R \mathrel{\ddot{\propto}} A$ and there is a bijection between A and A/R, then $R = \left\{(x, y) \in A^2 : x = y\right\}$.

> The statement is false. Consider $A = \mathbb{N}$ and R the equivalence relation s.t. A/R is the partition
>
> $$\{\{1\}, \{2, 3\}, \{4, 5, 6\}, \{7, 8, 9, 10\}, \ldots\}$$
>
> Then $F(1) = \{1\}, F(2) = \{2, 3\}, F(3) = \{4, 5, 6\}, \ldots$ is a bijection.
> It is interesting to study the finite case, however. If $A = \{a_1, \ldots, a_n\}$ a finite set,and F is bijective, we must have
>
> $$F(a_1) = X_1, \ldots, F(a_n) = X_n$$
>
> with $X_i \neq X_j$ for $i, j \in [1, n]$. In other words, $|A/R| = |A|$, which implies A/R is a partition of A into singleton sets. And because every element must be equivalent to itself, $A/R = \{\{a_1\}, \ldots, \{a_n\}\} \Rightarrow R = \left\{(x, y) \in A^2 : x = y\right\}$.

2.2 Functions with domain A/R

HAVING defined a space of equivalence class A/R, it is natural to study functions over this space. In general, functions of the form $f : A/R \mapsto B$ are ambiguous. For example, if we define $f(a/R) = f([a]) = a^2$ and R is the relationship "has the same parity", then the fact that $[2] = [4]$ would lead us to expect $f([2]) = 4 = f([4]) = 16$.

Notwithstanding, one of the fundamental ideas of modern algebra relates to a function of precisely this form:

Theorem 3. *If $f : A \mapsto B$ is onto, then $\overline{f}(a/ker\ f) = f(a)$ defines a bijection $\overline{f} : A/ker\ f \mapsto B$.*

Proof 3. *(Is a function)* Observe that $\overline{f}(a/ker\ f) = f(a)$ is uniquely determined for any $a \in A$.

(Injective) Let $a_1, a_2 \in A$ arbitrary elements with $a_1/ker\ f \neq a_2/ker\ f$. Assume $\overline{f}(a_1) = \overline{f}(a_2)$. Then $f(a_1) = f(a_2)$, which entails $(a_1, a_2) \in ker\ f$, which contradicts the assumption. Then $\overline{f}$ is injective.

(Surjective) Let $b \in B$ an arbitrary element. Since f is surjective, $b = f(a)$ for some $a \in A$. From this follows $b = \overline{f}(a/ker\ f)$.

Since $\overline{f}$ is injective and surjective, $\overline{f}$ is a bijection.

The theorem above guarantees, for any surjective f, the existence of a mapping from the quotient space $A/ker\ f$ onto I_f.

Problem 10. Say true, false or imprecise for the following statements.

(1) Let $R = \left\{(x, y) \in \mathbb{Z}^2 : 2 \mid x - y\right\}$. The equation $f(n/R) = \frac{1}{n^2+1}$ correctly defines a function.

False. Observe that

$$\mathbb{Z}/R = \{\{z \in \mathbb{Z} : z \text{ is even }\}, \{z \in \mathbb{Z} : z \text{ is odd }\}\}$$

We would then expect $f(0/R) = f(2/R) \iff 1 = \frac{1}{5}. (\perp)$

(2) If $R \ddot{\propto} A$ then $f : A/R \mapsto A$ defined as $f(a/R) = a$ is onto.

Imprecise because f is not necessarily a function and hence we cannot say it is onto.

3 Partial orders

Definition 6. If $R \propto A$ is reflexive, transitive and anti-symmetric, then it is a partial order.

We use $\leq$ to denote the binary relation that is a partial order. Because we define $\leq$ as a binary relation, we must emphasize that $\leq$ denotes a set of 2-uples. Furthermore, $<$ denotes $\{(a, b) \in \ \leq \ : a \leq b \wedge a \neq b\}$.

Definition 7. Let $\leq$ be a partial order over A. If $a < b$ and there is no z s.t. $a < z$ and $z < b$, then we write $a \prec b$ and read "b covers a" or "a is covered by b".

Observe that $\prec$ is itself the binary relation

$$\left\{(a, b) \in A^2 : a < b \wedge \neg \left(\exists z \in A : a < z \wedge z < b\right)\right\}$$

Definition 8. We say $\leq$ is a total order over A if it is a partial order s.t. $x \leq y$ or $y \leq x$ for any $x, y \in A$.

Partially or totally ordered sets are pairs $(P, \leq)$ where $\leq$ is a partial or total order (respectively) over P.

3.1 Maximum, minimum, maximal, minimal

Given a poset $(P, \leq)$, x is a maximum if $a \leq x$ for all $a \in P$. The definition of a minimum is analogous.

Theorem 4. *If $(P, \leq)$ a poset, then $(P, \leq)$ has at most one maximum.*

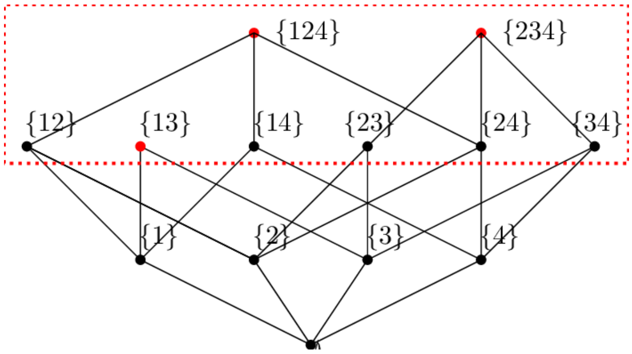
Proof 4. Assume $(P, \leq)$ is a poset with two distinct maximums x, y. By definition then $x \leq y$ and $y \leq x$. By anti-symmetry we have $x = y$, which is a contradiction.

Given a poset $(P, \leq)$, we use 1 to denote its maximum and 0 to denote its minimum, if they exist.

A maximal element of a poset $(P, \leq)$ is any $a \in P$ s.t. there is no $b \in P$ s.t. $a < b$. In other words, a maximal element is an element that has no successor in the order. Similarly, $a \in P$ is minimal if there is no $b \in P$ s.t. $b < a$. In other words, a minimal element is one that has no predecessor.

Problem 11. True or false: If $(P, \leq)$ a poset and $a \in P$ is not a maximum, then $a < b$ for some $p \in B$.

False. Consider any poset $(P, \leq)$ that has $n > 1$ maximals $m_1, \ldots, m_n$. Then, for any $i, j = 1, \ldots, n$, m_i is not a maximum (because $m_j \not< m_i$) but $m_i \not< b$ for all $b \in B$. For an example of a poset with $n = 3$ maximals, see the graph below.



Problem 12. True or false: If $(P, \leq)$ a poset without maximal elements, then P is infinite.

False, but only for a special case. If $P \neq \emptyset$, then it is true that for any $a_1 \in P$ there is some a_2 s.t. $a_1 < a_2$, and this extends to infinity: $a_1 < a_2 < \ldots$. However, if $P = \emptyset$, then the only binary relation over $\emptyset$ is $\emptyset^2 = \emptyset$, which gives the poset $(\emptyset, \emptyset)$. This poset is not only a partial order but a total order; it contains no maximal elements, and yet it is not infinite.

3.2 Supremum and infimum

Let $(P, \leq)$ a poset and $S \subseteq P$. We say $a \in P$ is an upper bound of S in $(P, \leq)$ when $b \leq a$ for all $b \in S$.

Note. $\emptyset \subseteq P$, so what's the deal? Well, every element in $\emptyset$ (which is no element at all) is lesser than any $a \in P$. In other words, every element in P is an upper bound of $\emptyset$.

Note 2. For any given $S \subseteq P$, many upper bounds may exist (see the previous note).

An element $a \in P$ is called the *supremum* of S in $(P, \leq)$ when two properties hold:

- a is an upper bound of S in $(P, \leq)$
- For any $b \in P$, if b is an upper bound of S in $(P, \leq)$, then $a \leq b$.

In other words, a is a supremum if it is the lesser upper bound. It is always unique.

Example. Let $(\mathbb{N}, \leq)$ denote the usual order over $\mathbb{N}$ and $S = \{1, 2, 3\}$. Any natural $n \geq 3$ is an upper bound of S in $(\mathbb{N}, \leq)$. However, 3 is the only supremum of S.

The definitions of the lower bound and the infimum are analogous. A lower bound of $S \subseteq P$ in $(P, \leq)$ is any $a \in P$ s.t. $a \leq b$ for all $b \in S$. The infimum is the greatest lower bound, or the lower bound a satisfying that any lower bound a' is s.t. $a' \leq a$.

Problem 13. Prove that if a, a' are supremums of S in $(P, \leq)$, then $a = a'$.

By definition, a, a' are the least upper bounds of S. If $a < a'$ then a' is no longer the least upper bound and hence $a' \leq a$. The same reasoning gives $a \leq a'$. Then, by anti-symmetry, $a = a'$.

The previous problem shows that we can speak of *the* supremum of $S \subseteq P$ for any poset $(P, \leq)$.

Problem 14. Let $(P, \leq)$ a poset.

(1) If $a \leq b$ then $\sup\{a, b\} = b$.

(2) Find $\{a \in P : a \text{ is upper bound of } \emptyset \text{ in } (P, \leq)\}$.

(3) If the supremum of $\emptyset$ in $(P, \leq)$ exists, it is a minimum element of $(P, \leq)$.

(1) The statement is trivially true.

(2) Assume $P \neq \emptyset$. Since $\emptyset \subseteq P$ it is correct to speak of the upper bound of $\emptyset$ in $(P, \leq)$. However, any element $a \in P$ is an upper bound of $\emptyset$ in $(P, \leq)$. The reason is that to prove $a \in P$ is *not* an upper bound of $\emptyset$, we should find some $x \in \emptyset$ s.t. $x \nleq a$—in other words, because the definition of upper bound involves a universal quantifier, its negation involves an existential, a counter-example. And since $\emptyset$ has no elements, there is no such counter-example. In conclusion,

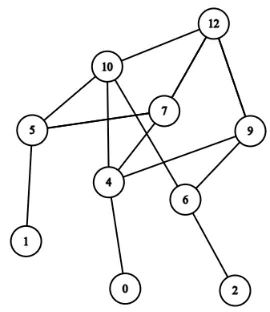
$$\{a \in P : a \text{ is upper bound of } \emptyset \text{ in } (P, \leq)\} = P$$

However, if $P = \emptyset$ (and therefore $\leq\ = \emptyset = \emptyset^2$), there is no upper bound of $\emptyset$ in $(\emptyset, \emptyset)$.

(3) Due to *(2)*, if the supremum exists then $P \neq \emptyset$. Then any $a \in P$ is an upper-bound of $\emptyset$, and the supremum is some $m \in P$ s.t. $m \leq a$ for any $a \in P$. $\therefore$ The supremum is the minimum of $(P, \leq)$.

Problem 15. Give a finite poset with three elements x_1, x_2, x_3 s.t. *(1)* $\{x_1, x_2, x_3\}$ is an anti-chain, meaning that $x_i \nleq x_j$ when $i \neq j$; *(2)* $\sup\{x_i, x_j\}$ doesn't exist for any $i \neq j$; *(3)* $\sup\{x_1, x_2, x_3\}$ exists.

A poset that satisfies this can be any that has the following Hasse diagram:



Here, $0, 1, 2$ are x_1, x_2, x_3. The supremum on any pair of them does not exist because each $\{x_i, x_j\}$ has two upper bounds that are not ordered with respect to one another. For example, the two smallest upper bounds of $\{1, 0\}$ are $10, 7$. But $10 \not\leq 7$ and $7 \not\leq 10$. However, $\sup\{0, 1, 2\} = 12$.

Problem 16. If $(P, \leq)$ a poset and $a = \sup(S)$ then $a = \sup(S \cup \{a\})$.

The statement is true. Our hypothesis is that $x \leq a$ for any $x \in S$, and $a \leq b$ for any upper-bound b of S. This evidently still holds for $S \cup \{a\}$, because $a \leq a$.

Problem 17. Let $(P, \leq)$ a poset and $a \in P$. Then a is a maximum of $(P, \leq)$ iff $a = \sup(P)$.

($\Rightarrow$) Assume a is a maximum of $(P, \leq)$. Then $x \leq a$ for all $x \in P$. Then a is an upper-bound of P. Furthermore, if there were some $u \in P$ s.t. u is an upper bound and $u < a$, then by definition u would not be an upper-bound of P because $a \not\leq u$. Then a is the least upper bound of P. ■

($\Leftarrow$) Assume a is the supremum of P. Then $x \leq a$ for all $x \in P$. The definition of a supremum of $S \subseteq P$ over $(P, \leq)$ requires that the supremum be an element of P. Then $a \in P$. Then by definition a is the maximum of P.

Note. The problem reveals a property; namely, that if $S \subseteq P$ and $\sup(S)$ over $(P, \leq)$ satisfies $\sup(S) \in S$, then this supremum is the maximum of $(S, \leq)$. Alternatively, this can be stated as follows: *The maximum of a poset $(P, \leq)$, if it exists, is the supremum m of P over $(P, \leq)$ whenever $m \in P$.*

Problem 18. Give true, false or imprecise.

(1) If $(P, \leq)$ a poset and $S \subseteq P$, then $a = \sup(S)$ in $(P, \leq)$ iff $a \in S$ and $b \leq a$, for all $b \in S$.

> False. It is not necessary that $\sup(S) \in S$. Consider the last graph we gave, where $\sup\{0, 1, 2\} = 12$ is not in $\{0, 1, 2\}$.

(2) Let $(P, \leq)$ a poset and $S \subseteq P$ and $a \in P$ an upper bound of S. If a is not the supremum of S, then there is some upper bound b of S s.t. $b < a$.

> The statement is false. If a is an upper bound of S but it is not the supremum, it could very well be the case that another upper bound b exists, with $a \nless b$ and $a \ngtr b$.
> For an example, go at the last graph we showed; imagine the maximum (i.e. 12) does not exist. Then consider that 10 is an upper bound of $\{0, 1\}$ but not a supremum, and yet there is no upper bound b of $\{0, 1\}$ s.t. $10 < b$.

Problem 19. Let $P = \{0\} \cup \{x \in \mathbb{R} : 1 < x \leq 2\}$. Let

$$\leq = \left\{(x, y) \in P^2 : x \leq y\right\}$$

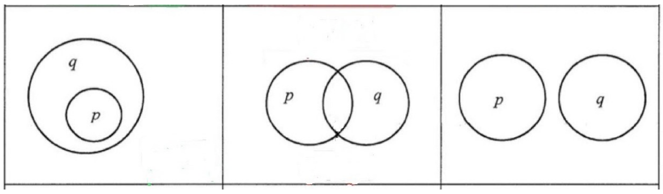
Let $S = \{x \in \mathbb{Q} : 1 < x \leq 2\}$. Does S have an infimum over $(P, \leq)$?

> The order is the usual order, but over $P = \{0\} \cup (1, 2]$. The set S (and in fact P as well) has only one lower bound over $(P, \leq)$; namely, 0. Observe that 1 is not a lower bound because $1 \notin P$, and there is no such thing as the "first rational number". Since 0 is the *only* lower bound it is also the greatest lower bound.

Problem 20. Say true or false. Let

$$\mathcal{D}((x_0, y_0), r) = \left\{(x, y) \in \mathbb{R}^2 : (x - x_0)^2 + (y - y_0)^2 \leq r^2\right\}$$

Let $P = \{\emptyset\} \cup \{\mathcal{D}((x_0, y_0), r) : x_0, y_0 \in \mathbb{R}, r > 0\}$. In the poset $(P, \subseteq)$, there is always $\inf\{D_1, D_2\}$, for any $D_1, D_2 \in P$.

> $\mathcal{D}((x_0, y_0), r)$ is the set of points within a circumference with center (x_0, y_0) and radius r. So P is the set of all disks, including $\emptyset$. Two disks may be related in one and only one of the ways schematized by the following Venn diagrams:
>
> 
>
>
> Formally, for $D_1, D_2 \in P$, the image depicts the following exhaustive and mutually exclusive cases:
>
> - $D_1 \subseteq D_2$,
> - $D_1 \cap D_2 \neq \emptyset$ but $D_1 \not\subseteq D_2$
> - $D_1 \cap D_2 = \emptyset$.
>
> It is easy to prove that in the first and third cases, there is an infimum. However, consider the case $D_1 \cap D_2 \neq \emptyset$ with $D_1 \not\subseteq D_2$. Let D_3 a disk s.t. $D_3 \subseteq D_1 \cap D_2$—this is, D_3 is an arbitrary, non-empty lower bound of $\{D_1, D_2\}$. Then, given any arbitrary $(z_1, z_2) \notin D_3$ that lies in $D_1 \cap D_2$, we can define $D_z = \mathcal{D}((z_1, z_2), \epsilon)$, with $\epsilon > 0$ a quantity sufficiently small to guarantee $D_z \cap D_3 = \emptyset$ and $D_z \in D_1 \cap D_2$. It is evident that D_z is a lower bound of $\{D_1, D_2\}$; but since $D_z \not\subseteq D_3$ we cannot say D_3 is the greatest lower bound.
>
> The argument above holds for any lower bound $D_3 \subseteq D_1 \cap D_2$. In general terms, we have shown that, in the case $D_1 \cap D_2 \neq \emptyset, D_1 \not\subseteq D_2$, for any lower bound D_3 of $\{D_1, D_2\}$, we can find a lower bound D_z that is not a subset of D_3. Therefore no greater lower bound exists and there is no infimum. Thus, the statement is false.

3.3 Poset homomorphism

Let $(P, \leq), (Q, \leq')$ two posets. A function $F : P \mapsto Q$ is called a homomorphism from $(P, \leq)$ to $(Q, \leq')$ iff

$$\forall x, y \in P : x \leq y \Rightarrow F(x) \leq' F(y)$$

We say F is an isomorphism of $(P, \leq)$ in $(Q, \leq')$ if F is a bijective homomorphism and F^{-1} is a homomorphism from $(Q, \leq')$ in $(P, \leq)$.

Note. Not all bijective homomorphism satisfy the last property. For example,

$$P = (\{1,2\}, \{(1,1),(2,2)\})$$
$$Q = (\{1,2\}, \{(1,2),(2,2),(1,2)\})$$

Then $F : \{1,2\} \mapsto \{1,2\}$ with $F(1) = 1, F(2) = 2$ is a bijective homomorphism. However, F^{-1} is not a homomorphism because $1 \leq' 2$ and $F^{-1}(1) = 1, F^{-1}(2) = 2, 1 \not\leq 2$.

The following theorem states that an isomorphism preserves all the properties of interest.

Theorem 5. *Let $(P, \leq), (Q, \leq')$ two posets. Assume F is an isomorphism from $(P, \leq)$ to $(Q, \leq')$. Then $x \leq y$ iff $F(x) \leq' F(y)$. Furthermore, if x is a maximum, a minimum, a maximal or a minimal of $(P, \leq)$, then $F(x)$ is that same thing of $(Q, \leq')$. Moreover, for any $x, y, z \in P$, $z = sup\{x, y\}$ if and only if $F(z) = sup\{F(x), F(y)\}$, and the same applies to the infimum. Lastly, $x \prec y$ if and only if $F(x) \prec' F(y)$.*

Proof 5. Complete.

Problem 21. Prove that if $(P, \leq), (Q, \leq')$ posets with an isomorphism F, then for all $x, y \in P$ we have $x < y \iff F(x) <' F(y)$.

($\Rightarrow$) Assume $x < y$. Then $F(x) \leq' F(y)$. Assume $F(x) = F(y)$. Then $F^{-1}(F(x)) = F^{-1}(F(y))$, which contradicts the assumption. Then $F(x) <' F(y)$.

($\Leftarrow$) Assume $F(x) <' F(y)$. Then we have $x \leq y$ (because F^{-1} is an homomorphism). If $x = y$ and $F(x) <' F(y)$, we have $F(y)$ covers $F(x)$ but y does not cover x ($\perp$). Then $x < y$.

Problem 22. Now prove x is a maximum iff $F(x)$ is a maximum.

($\Rightarrow$) Assume $x \in P$ is a maximum of $(P, \leq)$. Then $\forall y \in P : y \leq x$. Then $\forall y \in P : F(y) \leq' F(x)$. Then $F(x)$ is a maximum of $(Q, \leq')$.

($\Leftarrow$) Assume $F(x)$ is a maximum of $(Q, \leq')$ with $x \in P$. Then $\forall y \in P$: $F(y) \leq' F(x)$. Then $\forall y \in P : F^{-1}(F(y)) \leq F^{-1}(F(x))$ or rather $\forall y \in P : y \leq x$.

Problem 23. Now prove $x \prec y \iff F(x) \prec F(y)$.

Assume $x \prec y$ for $x, y \in P$. Then $y \leq x$ and for all $z \in P$ s.t. $y \leq z$ we have $x \leq z$. The first fact gives $F(y) \leq' F(x)$. The second fact gives $F(x) \leq F(z)$ for all $z \in P$ s.t. $y \leq z$. Then $F(x) \prec' F(y)$. The other side of the implication is left to the reader.

Problem 24. Give true, false or imprecise for the following statements.

(1) If $(P, \leq), (P, \leq')$ are finite and isomorphic, then $\leq = \leq'$.

True. Observe that $x \leq y \iff x \leq' y$ which by definition entails $(x, y) \in \leq \iff (x, y) \in \leq'$.

(2) If $(P, \leq)$ a poset s.t. every $F : P \mapsto P$ is homomorphic from $(P, \leq)$ in $(P, \leq)$, then $|P| = 1$.

> False. Assume $P = \emptyset$. There is only one function $F : P \to P$, namely $\emptyset^2 = \emptyset$. This function is a homomorphism because no counter-example can be found to the defining properties of a homomorphism in the empty set. So $P = \emptyset$ satisfies the properties but $|P| \neq 1$.

3.4 Lattices

A poset $(P, \leq)$ is called a lattice if for any $x, y \in P$, $\sup\{x, y\}$ and $\inf\{x, y\}$ exist. Informally, this means that any pair of elements in P is related to some common successor and some common predecessor in P. We use $(L, \leq)$ to denote a lattice.

Problem 25. Prove that $(\mathbb{N}, |)$ is a lattice. Does it have maximum and minimum?

We skip the proof that $(\mathbb{N}, |)$ is a poset. Let $n_1, n_2 \in \mathbb{N}$ two arbitrary numbers. Because the set $\mathcal{D}(n_1, n_2) = \{d \in \mathbb{N} : d \mid n_1, d \mid n_2\}$ is a finite set over the natural numbers, it has a maximum. Of course, from a lattice perspective, $\mathcal{D}(n_1, n_2)$ is the set of lower bounds of $\{n_1, n_2\}$. Then $\inf\{n_1, n_2\} = \max \mathcal{D}(n_1, n_2)$ is guaranteed to exist. The proof that $\sup\{n_1, n_2\}$ exists is similar.

Because $1 \mid n$ for any $n \in \mathbb{N}$, 1 is a minimum. However, there is no natural $m \in \mathbb{N}$ s.t. $n \mid m$ for every n, so the set lacks a maximum.

Problem 26. Show that if $(P, \leq)$ is a total order then it is lattice.

Assume $(P, \leq)$ is a total order. If $\ldots \leq p_0 \leq p_1 \leq p_2 < \ldots$ is the (potentially infinite) order of P, then for any $i, k \in \omega$, $\sup\{p_i, p_{i+k}\} = p_{i+k}$ and $\inf\{p_i, p_{i+k}\} = p_i$. Then $(P, \leq)$ is a lattice.

Problem 27. If $(P, \leq)$ a lattice then $\sup(S)$ exists for any $S \subseteq P$?

The statement is false. $(\mathbb{N}, \leq)$ with $\leq$ the usual order is a total order and therefore a lattice, and $\sup(\mathbb{N})$ does not exist.

Problem 28. True or false: If $(P, \leq)$ a lattice and $S \subseteq P$, then $(S, \leq \cap S^2)$ is a lattice.

False. Consider as a counter example $(\{1, 2, 3, 6\}, |)$. It is evident that this is a lattice, and here

$$| \; = \{(1,2), (1,3), (1,6), (2,6), (3,6)\}$$

Now consider $(\{1, 2, 3\}, \{(1,2), (1,3)\})$. This is obviously not a lattice.

Problem 29. True or false: If $(P, \leq)$ a lattice and $S \subseteq P$ non-empty and s.t. $(S, \leq \cap S^2)$ a lattice, then for any $a, b \in S$, $\inf\{a, b\}$ in $(P, \leq)$ coincides with $\inf\{a, b\}$ in $(S, \leq \cap S^2)$.

Should be true. COMPLETE.

Problem 30. Let $P \subseteq \mathcal{P}(\mathbb{N})$ and assume $(P, \leq)$ a lattice with

$$\leq \ = \{(A, B) \in P \times P : A \subseteq B\}$$

Is $\inf\{A, B\} = A \ \cap|_{P^2} B$?

Since $(P, \leq)$ a lattice we know the infimum of any pair of elements always exist. Let $A, B \in P$ and assume $\inf\{A, B\} = I$. Then, by definition, $I \subseteq A$ and $I \subseteq B$. Furthermore, for any $I' \in P$ s.t. $I' \subseteq A$ and $I' \subseteq B$ we have $I' \subseteq I$. It follows that for every $x \in A \cap B$ we have $x \in I$. Then $I = A \cap B$. And since we have imposed the condition $A, B \in P$, the restriction of the intersection to P^2 satisfies what we have shown. The statement is true.

Problem 31. If $(P, \leq)$ a lattice and m is a maximal element of $(P, \leq)$, then m is a maximum of $(P, \leq)$. Is this true if $(P, \leq)$ is not a lattice?

The statement is true. Assume m is not a maximum. Then either there is some $m' \in P$ s.t. $m \leq m', m \neq m'$, or there is some $x \in P$ s.t. $x \not\leq m$. If the first case holds then m is not maximal $(\perp)$. If the second case holds then $\sup\{x, m\}$ does not exist and $(P, \leq)$ is not a lattice $(\perp)$. Then m is a maximum. ∎

3.5 Binary operations

Given a set A, a binary operation over A is a function $f : A^2 \to A$ s.t. $\mathcal{D}_f = A^2$. A lattice has by definition two binary operations: inf and sup. We will write $a \vee b$ and $a \wedge b$ to denote the supremum and infimum of $\{a, b\} \subseteq P$, respectively.

Some properties with their proofs: Assume $x, y \in (L, \leq)$ a lattice.

(1) $x \leq x \vee y$

Proof. $x \leq x \vee y$ by definition of supremum, because $x \vee y$ is the least $z \in L$ s.t. $x \leq z, y \leq z$.

(2) $x \wedge y \leq x$

Proof. The proof is similar to the previous case.

(3) $x \vee x = x$

Proof. $\sup\{x, x\} = \sup\{x\}$ and of course x is the lesser element in L s.t. $x \leq x$.

(4) $x \wedge x = x$

Proof. Similar to the previous case.

(5) $x \vee y = y \vee x$

Proof. Trivial; left to the reader.

(6) $x \wedge y = y \wedge x$

Theorem 6. *Let* $(L, \leq)$ *a lattice. For any* $x, y \in L$*, we have* $x \leq y \iff x \vee y = y$*. Furthermore,* $x \leq y \iff x \wedge y = x$*.*

Proof 6. Complete.

Theorem 7 (Absortion laws)**.** *Let* $(L, \leq)$ *a lattice and* $x, y, z \in L$*. Then (1)* $x \vee (x \wedge y) = x$ *and (2)* $x \wedge (x \vee y) = x$*.*

Proof 7. Complete.

Theorem 8 (Order preservation)**.** *If* $x \leq z$ *and* $y \leq w$*, then* $x \circ y \leq z \circ w$*, with* $\circ \in \{\vee, \wedge\}$*.*

Proof 8. Complete.

Some proving tips.

- If you want to prove $x \vee y \leq z$, it suffices to show $x \leq z$ and $y \leq z$.

  Justification. Assume $x \leq z, y \leq z$. Then z is an upper bound of $\{x, y\}$. Since $x \vee y$ is the least upper bound, $x \vee y \leq z$.

- If you want to prove $z \leq x \wedge y$, it suffices to show $z \leq x$ and $z \leq y$.

  Justification. If $z \leq x, z \leq y$, then z is a lower bound of $\{x, y\}$. Then, because $x \wedge y$ is the least lower bound of this set, $z \leq x \wedge y$.

Theorem 9 (Associativity)**.** *For any* $x, y, z \in L$ *with* $(L, \leq)$ *a lattice,* $(x \vee y) \vee z = x \vee (y \vee z)$*, and the same holds for* $\wedge$*.*

Proof 9. *(1)* Firstly, we will prove $(x \vee y) \vee z \leq x \vee (y \vee z)$. To do this, we will prove the expression to the right is an upper-bound of the terms in the expressions to the left.

(1.1) It follows directly from the definition of supremum that $x \leq x \vee (y \vee z)$. Furthermore, let $\varphi = y \vee z$, so that by definition $y \leq \varphi$. Since $\varphi \leq x \vee \varphi$ we have $y \leq x \vee \varphi$ by transitivity. In other words, $y \leq x \vee (y \vee z)$. Then $x \vee (y \vee z)$ is an upper bound of $\{x, y\}$. Then $x \vee y \leq x \vee (y \vee z)$.
(1. 2) That $z \leq x \vee (y \vee z)$ is clear from the fact that $z \leq y \vee z$ and $y \vee z \leq x \vee (y \vee z)$ (apply transitivity).

From *(1.1, 1.2)* follows that $x \vee (y \vee z)$ is an upper bound of $\{x \vee y, z\}$. Then $(x \vee y) \vee z \leq x \vee (y \vee z)$. ■

(2) In a similar way, we can prove that $x \vee (y \vee z) \leq (x \vee y) \vee z$. Since $\varphi \leq \psi$ and $\psi \leq \varphi$ imply $\varphi = \psi$ for any $\varphi, \psi \in L$, this concludes the proof.

Theorem 10. *If* $(L, \leq)$ *a lattice and* $x, y, z \in L$*, then* $(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee z)$*.*

Proof 10. *(1)* Observe that $(x \wedge y) \vee (x \wedge z) \leq x$. The reason is that $x \wedge y \leq x$ trivially, $x \wedge z \leq x$ trivially, and therefore x is an upper bound of $\{x \wedge y, x \wedge z\}$. Then the supremum of this set is necessarily less than or equal to x.

(2) Observe that $(x \wedge y) \vee (x \wedge z) \leq y \vee z$. The reason is that $x \wedge y \leq y \leq y \vee z$ and $x \wedge z \leq z \leq y \vee z$. Then $y \vee z$ is an upper bound of $\{x \wedge y, x \wedge z\}$, and then the supremum of this set is less than or equal to $y \vee z$.

(3) Results *(1)* and *(2)* entail $(x \wedge y) \vee (x \wedge z)$ is a lower bound of $\{x, y \vee z\}$. Then $(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee z)$.

Using the same tricks we can prove $x \wedge (y \vee z) \leq (x \wedge y) \vee (x \wedge z)$, which completes the proof. ∎

4 Lattices as algebras

We have treated lattices as a special kind of poset. However, a lattice can be modeled as a special kind of algebra. In general, a lattice is any 3-uple $(L, \vee, \wedge)$ with L a set and $\vee, \wedge$ binary relations over L that satisfy the following properties:

For any $x, y, z \in L$:

- $x \vee x = x \wedge x$
- $x \vee y = y \vee x$ (Commutativity)
- $x \wedge y = y \wedge x$ (Commutativity)
- $(x \vee y) \vee z = x \vee (y \vee z)$ (Associativity)
- $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ (Associativity)
- $x \vee (x \wedge y) = x$
- $x \wedge (x \vee y) = x$

Viewed in this way, if $(L, \leq)$ a lattice *in the poset* sense, then we have $(L, \vee, \wedge)$ a lattice *in the algebraice sense* where $\vee, \wedge$ denote the supremum and infimum operators. More formally,

Theorem 11 (Dedekind). *If* $(L, \vee, \wedge)$ *a lattice, the binary relation* $x \leq y \iff x \vee y = y$ *is a partial order over L and it satisfies sup* $\{x, y\} = x \vee y$, *inf* $\{x, y\} = x \wedge y$, *for any* $x, y \in L$.

Proof 11. Complete.

Note. The theorem above states that any lattice in the algebraic sense *induces* a lattice in the poset sense. The *operations* which define the algebra induce a partial order where these operations correspond to the supremum and minimum.

We call $\leq$ the partial order induced by $(L, \vee, \wedge)$ and $(L, \leq)$ the poset induced by $(L, \vee, \wedge)$.

Problem 32. Compute the cardinality of the set

$$S = \{(\{1, 2, 3\}, \vee, \wedge) : (\{1, 2, 3\}, \vee, \wedge) \text{ is a lattice}\}$$

The set consists of all possible lattices (in the algebraic sense) over $\{1, 2, 3\}$, and thus we are interested in finding how many possible such lattices are there. Dedekind's theorem states that any such lattice induces a lattice partial order $\leq$ s.t. $(P, \leq)$ is a partial order and $a \leq b \iff a \vee b = b$. Thus, the question becomes how many lattice partial orders exist over $\{1, 2, 3\}$. There are $3! = 6$ total orders that are evidently lattices.

The partial orders are of two kinds: no element is in relation to another, and one element is not in relation to the others. In the first case, the supremum between two elements does not exist and the poset is not a lattice. In the second case, the supremum between the isolated element and any of the others does not exist.

$\therefore$ There are $3! = 6$ lattices over a set of 3 elements, and $|S| = 6$.

Problem 33. If $(L, \vee, \wedge)$ is a lattice then $(L, \wedge, \vee)$ is a lattice. What is the relation between the posets induced by them?

The lattice poset induced by the first lattice satisfies $x \leq y \iff x \vee y = y$, while the one induced by the second lattice satisfies $x \leq y \iff x \vee y = x$. So the ordering between the two posets is inverse; i.e. if $a \leq_1 b$ then $b \leq_2 a$. The Hasse diagrams of these posets will be horizontal mirrors of each other.

Problem 34. True, false or imprecise: If $(L, \vee, \wedge)$ a lattice and $t \in \vee$, then $Ti(t) =$ 3-UPLE.

$\vee$ is a function; i.e. a set of 2-uples. So if $t \in \vee$ we have $Ti(t) =$ 2-uple. The statement is false.

Problem 35. True, false or imprecise: If $(L, \vee, \vee)$ a lattice, then L has exactly one element.

False. $(\emptyset, \vee, \vee)$ is a lattice for any function $\vee$, but $|\emptyset| \neq 1$. Only if we assume $L \neq \emptyset$ can we say the statement is true. And this because if more than one element existed, we would require that any pair $x \neq y$ in the induced lattice poset satisfies $\sup\{x, y\} = x \iff \inf\{x, y\} = y$. But if the functions inducing the supremum and infimum are the same, this would entail $x \vee y = x$ and $x \vee y = y$, which in turn implies $y \leq x$ and $x \leq y$. But then $\leq$ is not anti-symmetric, which contradicts that $(L, \leq)$ is a lattice.

Problem 36. True, false or imprecise: If $(L, \vee, \wedge)$ a lattice, then it is always the case that $\wedge \leq \vee$.

The statement is equivalent to $(\vee, \wedge) \in \{(x, y) : x \vee y = y\} \subseteq L^2$. But clearly $\vee \notin L, \wedge \notin L$. The statement is false.

Problem 37. True, false or imprecise: If $(L, \vee, \wedge)$ a lattice, then $\vee(x, y, z) = \wedge(x, y, z)$ for any $x, y, z \in L$.

Imprecise. There are no 3-argument functions $\vee, \wedge$ defined in this context.

4.1 Distributive lattice

A lattice $(L, \vee, \wedge)$ is said to be distributive when, for any $x, y, z, \in L$, we have $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$. It can be proven that if this property holds (distributivity of $\wedge$ over $\vee$), its complementary property holds (distributivity of $\vee$ over $\wedge$).

Problem 38. Prove that $(\mathbb{R}, \max, \min)$ and $(\mathcal{P}(\mathbb{N}), \cup, \cap)$ are distributive.

(1) We skip the proof that $(\mathbb{R}, \max, \min)$ is a lattice. Let $\wedge, \vee$ denote min and max. Let $u = x \vee y$ and $w = z \wedge u$. Let us examine the cases where $x \leq y$ and $y < x$, and let us use A and B to denote the expressions of the distributive property.

$(x \leq y)$ Here $A = x \wedge (y \vee z) = x$, because $x \leq y \leq y \vee z$. At the same time, $B = x \vee (x \wedge z) = x$ because $x \geq (x \wedge z)$. $\therefore A = B$. ■

$(y < x)$ Again, two cases.

- $(x \leq z)$ Here $y < x \leq z$. Then $A = x \wedge y = x$ and $B = y \vee x = x$. $\therefore A = B$.
- $(z \leq x)$ Here $A = x \wedge (y \vee z) = y \vee z$. Simultaneously, $B = y \vee z$. So $A = B$.

(2) We will again inspect two cases given $A, B, C \in \mathcal{P}(\mathbb{N})$. Observe that the order induced by these operations is $\subseteq$, since $A \leq B \iff A \cup B = B$, and $A \leq B \iff A \cap B = A$. We will use φ, ψ to denote the sides of the distributive property.

$(A \subseteq B)$ Since $A \subseteq B \subseteq (B \cup C)$, we have $A \subseteq (B \cup C)$ and

$$\begin{aligned} A &= A \cap (B \cup C) \\ &= A \end{aligned}$$

Furthermore, $(A \cap B) \cup (A \cap C) = A \cup (A \cap C) = A$. Then $\varphi = \psi$.

$(B \subseteq A)$ Similar to the previous excercise. COMPLETE.

4.2 Sub-lattices and sub-universes

If $(L, \wedge, \vee), (L', \wedge', \vee')$ are lattices, we say the first is a sub-lattice of the other iff

- $L \subseteq L'$
- $\vee = \vee' |_{L \times L}$ and $\wedge = \wedge' |_{L \times L}$

We say $S \subseteq L$ is a sub-universe of $(L, \vee, \wedge)$ if $S \neq \emptyset$ and S is closed under $\vee, \wedge$.

Note. The concepts of sub-lattice and sub-universe are similar but not identical. A sub-universe of $(L, \vee, \wedge)$ is a *set*; a sub-lattice of $(L, \vee, \wedge)$ is a lattice. It is true that if S is a sub-universe, then $(S, \vee|_{S\times S}, \wedge|_{S\times S})$ is a sub-lattice, and that every sub-lattice is obtained in this manner. In other words, there is a bijection between sub-lattices and sub-universes.

Problem 39. What are the sub-universes of:

(1) $(\mathcal{P}(\{1, 2\}, \cup, \cap))$

(2) $(\{1, 2, 3, 6, 12\}, \gcd, \operatorname{lcm})$

(3) $(\mathbb{R}, \max, \min)$

(1) A sub-universe of a poset is a non-empty subset of the poset that is closed under $\wedge, \vee$. Since $\{1, 2\}$ has two elements, no strict subset of it is a sub-universe. $\therefore$ $\{1, 2\}$ is the only sub-universe of $\{1, 2\}$.

(2) The only subset which is not a sub-universe is $\{2, 3\}$, (the primes) since $\gcd(2, 3) = 1$. Any other subset contains either a prime in $\{2, 3\}$ with non-prime numbers, or only non-prime numbers. It is easy to see that the subsets with non-prime numbers only,

$$\{12, 6\}, \{12, 6, 1\}, \{1, 6\}, \{1, 12\}$$

are closed under gcd and lcm. The sets containing a prime among other elements are also cloesd. So the sub-universes of the set $S = \{1, 2, 3, 6, 12\}$ are $U = \{W \in \mathcal{P}(S) : W \neq \{2, 3\} \wedge |W| > 1\}$.

(3) Every subset $S \subseteq \mathbb{R}$ with $|S| > 1$ is closed under max and min. Then the sub-universes of this poset are all possible sets of real numbers with more than one element.

4.3 Lattice homomorphisms and isomorphisms

Let $(L, \vee, \wedge)$, $(L', \vee', \wedge')$ be lattices. A function $F : L \mapsto L'$ is a lattice homomorphism from $(L, \vee, \wedge)$ in $(L', \vee', \wedge')$ iff

$$F(x \circ y) = F(x) \circ' F(y)$$

with $\circ$ either $\vee$ or $\wedge$. A homomorphism is called an isomorphism when it is bijective and its inverse is a homomorphism as well. We write $(L, \wedge, \vee) \simeq (L', \wedge', \vee')$ to say that two lattices are isomorphic.

Theorem 12. *If F is a bijective homomorphism between two lattices, then it is an isomorphism.*

Proof 12. Assume F a bijective homomorphism. Observe that, since F is a homomorphism,

$$\begin{aligned} F\left[F^{-1}(x) \circ F^{-1}(y)\right] &= F\left[F^{-1}(x)\right] \circ' F\left[F^{-1}(y)\right] \\ &= x \circ' y \end{aligned}$$

It follows that

$$F^{-1}\left[x \circ' y\right] = F^{-1}\left[F\left(F^{-1}(x) \circ F^{-1}(y)\right)\right] = F^{-1}(x) \circ F^{-1}(y)$$

■

Theorem 13. *Let F an homomorphism from* $(L, \vee, \wedge)$ *in* $(L', \vee', \wedge')$. *Then* I_F *is a sub-universe of* $(L', \vee', \wedge')$, *and in consequence F is an homomorphism from* $(L, \vee, \wedge)$ *in* $(I_F, \vee' |_{I_F \times I_F}, \wedge' |_{I_F \times I_F})$.

Proof 13. Complete

Theorem 14. *Let* $(L, \vee, \wedge)$ *and* $(L', \vee', \wedge')$ *lattices with associated posets* $(L, \leq), (L', \leq')$. *Then* F *is an isomorphism of* $(L, \vee, \wedge)$ *in* $(L', \vee', \wedge')$ *iff* F *is an isomorphism from* $(L, \leq)$ *to* $(L', \leq')$.

Proof 14. Complete

4.4 Lattice congruence

A congruence over a lattice $(L, \vee, \wedge)$ is an equivalence relation $\theta \ddot{\propto} L$ s.t.

$$x_1 \theta x_2 \text{ and } y_1 \theta y_2 \Rightarrow (x_1 \vee y_1)\theta(x_2 \vee y_2) \text{ and } (x_1 \wedge y_1)\theta(x_2 \theta y_2)$$

This condition essentially requires that equivalence is preserved in the lattice operations; i.e. the supremum/infimum between members of two classes should be equivalent to the supremum/infimum between any other members of those two classes.

Because equivalence is preserved among the classes of equivalence in the lattice operations, it is possible to define the supremum/infimum between two classes:

$$x/\theta \,\widetilde{\circ}\, y/\theta = (x \circ y)/\theta$$

with $\circ \in \{\vee, \wedge\}$.

Example. *(1)* Consider the lattice $(\{1,2,3,4,5,6\}, \max, \min)$. Let θ be the equivalence relation induced by the partition $\{\{1,2\},\{3\},\{4,5\}\}$. Then θ is a congruence. For example,

$$1\theta 2, 4\theta 5 \text{ and } (1 \max 4)\theta(2 \max 5)$$

The same can be verified for the min operation. Of course, we have that $\{1,2\} \widetilde{\max} \{4,5\} = (1 \max 4)/\theta = 4/\theta = \{4,5\}$.

Theorem 15. *If $(L, \vee, \wedge)$ a lattice and θ a congruence relation of this lattice, then $(L/\theta, \widetilde{\vee}, \widetilde{\wedge})$ is a lattice.*

We use $\widetilde{\leq}$ to denote the partial order associated to the lattice $(L/\theta, \widetilde{\vee}, \widetilde{\wedge})$.

Proof 15. Since $(L, \vee, \wedge)$ is a lattice, $x \vee y = x \wedge y$. By definition,

$$[x]\widetilde{\vee}[y] = [(x \vee y)] = [(x \wedge y)] = [x]\widetilde{\wedge}[y]$$

Commutativity is similar (we give it only for $\widetilde{\vee}$):

$$[x]\widetilde{\vee}[y] = [(x \vee y)] = [(y \vee x)] = [y]\widetilde{\vee}[x]$$

Associativity (we give it only for $\widetilde{\vee}$):

$$\begin{aligned} ([x]\widetilde{\vee}[y])\widetilde{\vee}[z] &= [(x \vee y)]\,\widetilde{\vee}[z] \\ &= [(x \vee y) \vee z] \\ &= [x \vee (ylorz)] \\ &= [x]\widetilde{\vee}\left([y]\widetilde{\vee}[z]\right) \end{aligned}$$

Now we will prove $[x]\widetilde{\vee}([x]\widetilde{\wedge}[y]) = [x]$. But this can be done with words. The infimum $[x]\widetilde{\wedge}[y]$ will be the equivalence class of the infimum between x and y in the original lattice. If the result is $[x]$ then the property follows immediately. If the result is $[y]$ we have $y \wedge x = y \Rightarrow y \vee x = x$ which entails $[x]\widetilde{\vee}[y] = [x]$.
Then $(L/\theta, \widetilde{\wedge}, \widetilde{\vee})$ is a lattice. ■

Theorem 16. *If $(L, \vee, \wedge)$ a lattice and θ a congruence over this lattice, then*

$$x/\theta \,\widetilde{\leq} y/\theta \iff y\theta(x \vee y)$$

for any $x, y \in L$.

Proof 16. Recall that the order induced by a lattice $(L, \vee, \wedge)$ is $x \leq y \iff x \vee y = y$. So to prove this theorem we must study the order induced by $(L/\theta, \widetilde{\wedge}, \widetilde{\vee})$; namely,

$$[x]\widetilde{\leq}[y] \iff [x]\widetilde{\vee}[y] = [y]$$

It is clear that if $[x]\widetilde{\vee}[y] = [y]$ we have $[(x \vee y)] = [y]$, which is exactly the same as saying $(x \vee y)\theta y$. ■

Theorem 17. *If* $F : (L, \wedge, \vee) \mapsto (L', \wedge', \vee')$ *an homomorphism, then* $ker(F)$ *is a congruence over* $(L, \wedge, \vee)$.

Proof 17. Let $\theta = ker(F)$ with F a homomorphism between two arbitrary lattices $(L, \wedge, \vee)$, $(L', \wedge', \vee')$. If $\theta = \emptyset$ then θ is a congruence by lack of counter-examples. Assume $\theta \neq \emptyset$.

Let x_0, x_1, y_0, y_1 be elements of L s.t. $x_0 \theta x_1$ and $y_0 \theta y_1$. Then $F(x_0) = F(x_1)$ and $F(y_0) = F(y_1)$. Since $x_0 \circ x_1 \in \{x_0, x_1\}$, we have $F(x_0 \circ x_1) = F(x_0)$, and $F(y_0 \circ y_1) = F(y_0)$.

We know $F(x_0 \circ y_0) \in \{F(x_0), F(y_0)\}$, and $F(x_1 \circ y_1) \in \{F(x_1), F(y_1)\}$. We wish to prove $F(x_0 \circ y_0) \neq F(x_1 \circ y_1)$. The only problematic case is when the first expression is $F(x_0)$ and the latter $F(y_1)$ or vice-versa.

Assume without loss of generality that $\circ = \vee$ and

$$\textit{(1)}\ F(x_0 \circ y_0) = F(x_0)$$
$$\textit{(2)}\ F(x_1 \circ y_1) = F(y_1)$$

Prop. *(1)* entails $(x_0 \vee y_0)\theta x_0$. Then, in the order induced by θ, $[y_0] \tilde{\leq} [x_0]$. But $[y_0] = [y_1], [x_0] = [x_1]$, and then $[y_1] \tilde{\leq} [x_1]$. But then $(y_1 \vee x_1)\theta x_1$.

$\therefore F(y_1 \vee x_1) = F(x_1)$ and *(2)* gives $F(x_1) = F(y_1)$.

$\therefore F(x_0) = F(x_1) = F(y_1)$ and *(1)* and *(2)* give $F(x_0 \vee y_0) = F(x_1 \vee y_1)$.

■

Theorem 18. *Let* $(L, \vee, \wedge)$ *a lattice and* θ *a congruence over it. Then* π_θ *is a homomorphism from* $(L, \vee, \wedge)$ *to* $(L/\theta, \widetilde{\vee}, \widetilde{\wedge})$*, and* $\ker(\pi_\theta) = \theta$.

Proof 18. Let $x, y \in L$. Then

$$\pi_\theta(x \circ y) = (x \circ y)/\theta = x/\theta \,\widetilde{\circ}\, y/\theta = \pi_\theta(x) \,\widetilde{\circ}\, \pi_\theta(y)$$

Now, $\ker(\pi_\theta) = \left\{(a, b) \in \mathcal{D}^2_{\pi_\theta} : \pi_\theta(a) = \pi_\theta(b)\right\}$. Since π_θ is a homomorphism, $\mathcal{D}_{\pi_\theta} = L$, and due to the definition of canonic projection, $\pi_\theta(x) = \pi_\theta(y) \iff x\theta y$. Then $\ker(\pi_\theta) = \{(a, b) \in L : a\theta b\}$. This is trivially equal to θ.

Problem 40. Give all the congruences of $(\{1, 2, 3, 6, 12\}, \gcd, \text{lcm})$.

Complete.

Problem 41. Let θ a congruence over $(L, \vee, \wedge)$. Prove that, if $c \in L/\theta$,

(1) c is a sub-universe of the lattice.

(2) c is a convex subset of the lattice; i.e. for any $x, y, z \in L$

$$x, y \in c \text{ and } x \leq z \leq y \Rightarrow z \in c$$

(1) A sub-universe is a non-empty subset of a lattice that is closed under the lattice operations. That $c/\theta \subseteq L$ is trivial, and it must be non-empty because each element is at least equivalent to itself. Assume it is not closed under the lattice operations; i.e. assume there are $x_0, x_1 \in c/\theta$ s.t. $u = x_0 \circ x_1 \notin c/\theta$.

Theorem **18** ensures that π_θ is a homomorphism from $(L, \vee, \wedge)$ to $(L/\theta, \widetilde{\vee}, \widetilde{\wedge})$. But by assumption:

$$\pi_\theta(x_0 \circ x_1) \neq c/\theta \Rightarrow \pi_\theta(x_0) \mathbin{\widetilde{\circ}} \pi_\theta(x_1) \neq c/\theta$$

But this entails $c/\theta \mathbin{\widetilde{\circ}} c/\theta \neq c/\theta$, which is absurd because $(L/\theta, \widetilde{\vee}, \widetilde{\wedge})$ is a lattice. Then c/θ must be closed and hence must be a sub-universe. ■

(2) Let $x, y, z \in L$. Assume $x, y \in c$ and $x \leq z \leq y$. We wish to prove this entails $z \in c$.

Since $(L/\theta, \widetilde{\wedge}, \widetilde{\vee})$ is a lattice (**Theorem 15**), it induces a poset $(L, \widetilde{\leq})$ s.t.

$$a \widetilde{\leq} b \iff b\theta(a \widetilde{\vee} b)$$

Since $x \leq z \leq y$ we have

1. $z\theta(x \vee z)$
2. $y\theta(z \vee y)$

In terms of the homomorphism π_θ, this means

1. $\pi_\theta(z) = \pi_\theta(x) \widetilde{\vee} \pi_\theta(z)$
2. $\pi_\theta(y) = \pi_\theta(z) \widetilde{\vee} \pi_\theta(y)$

Since $x, y \in c$ we have $\pi_\theta(x) = \pi_\theta(y)$. If we look at equations (1) and (2), this entails $\pi_\theta(z) = \pi_\theta(y)$.

$\therefore z \in c$.

Problem 42. Say true, false or imprecise for the following statements, where $(L, \vee, \wedge)$ is a lattice.

(1) Let S a sub-universe of the lattice and θ a congruence of $(S, \vee_{S\times S}, \wedge_{S\times S})$. There is a congruence λ of $(L, \vee, \wedge)$ s.t. $\theta = \lambda \cap S^2$.

False. See the *Congruence extension property.*

(2) Assume the lattice is distributive and θ is a congruence over it. Then $(L/\theta, \widetilde{\vee}, \widetilde{\wedge})$ is distributive.

The statement is true. Observe that for $x, y, z \in L$,

$$\begin{aligned} x/\theta \widetilde{\vee} (y/\theta \widetilde{\wedge} z/\theta) &= x/\theta \widetilde{\vee} \left((y \wedge z) / \theta \right) \\ &= \left(x \vee (y \wedge z) \right) / \theta \\ &= \left((x \vee y) \wedge (x \vee z) \right) / \theta \\ &= (x \vee y) / \theta \widetilde{\wedge} (x \vee z) / \theta \\ &= \left(x/\theta \widetilde{\vee} y/\theta \right) \widetilde{\wedge} \left(x/\theta \widetilde{\vee} z/\theta \right) \end{aligned}$$

(3) Let θ a congruence over the lattice. If $u \in L$ is s.t. u/θ is a maximum of $(L, \vee, \wedge)/\theta$, then u is a maximum of the original lattice.

The statement is imprecise. The symbol $(L, \vee, \wedge)/\theta$ is undefined.

Problem 43. Let $(L, \vee, \wedge)$ a lattice, θ a congruence over it and $\leq$ the order induced by $\vee$. Let $(L/\theta, \widetilde{\vee}, \widetilde{\wedge})$ the quotient lattice and $\widetilde{\leq}$ the order induced by $\widetilde{\vee}$. Prove that given $c_0, c_1 \in L/\theta$, $c_0 \widetilde{\leq} c_1$ iff there are $x \in c_0, y \in c_1$ s.t. $x \leq y$.

($\Rightarrow$) Assume there are $c_0, c_1 \in L/\theta$ s.t. $c_0 \widetilde{\leq} c_1$. There must be elements x, y s.t. $x/\theta = c_0$ and $y/\theta = c_1$. By **Theorem 16** we have

$$y\theta(x \vee y) \tag{1}$$

If $x = y$ then $x \leq y$ and the result is trivial, so assume $x \neq y$. Then $c_0 \neq c_1$. If $x \vee y = x$, equation (1) gives $y\theta x$, which violates the fact that $c_0 \neq c_1$. So $x \vee y = y$.

$\therefore x \leq y$.

($\Leftarrow$) Assume there are $x \in c_0, y \in c_1$ s.t. $x \leq y$. Then $x \vee y = y$ and trivially $y\theta(x \vee y)$. Then, by **Theorem 16**, we have $x/\theta \leq y/\theta$.

$\therefore c_0 \leq c_1$

5 Bounded and complemented lattices

5.1 Bounded sub-lattices

A bounded lattice restricts the notion of lattice to those whose elements are bounded, in the supremum and infimum operations, by special elements 0 and 1.

Definition 9. A bounded lattice is a 5-upla $(L, \vee, \wedge, 0, 1)$ s.t. $(L, \vee, \wedge)$ is a lattice, $0, 1 \in L$, and $\forall x \in L$:

1. $0 \vee x = x$
2. $1 \vee x = 1$

Definition 10. Given $(L, \vee, \wedge, 0, 1)$ and $(L', \vee', \wedge', 0', 1')$ two bounded lattices, we say the first is a sub-lattice of the latter if the following conditions hold:

1. $L \subseteq L'$
2. $0 = 0', 1 = 1'$
3. $\circ = \circ'_{L \times L}$

We define a sub-universe of a bounded lattice in a way similar to the sub-universe of any lattice.

Definition 11. Let $(L, \vee, \wedge, 0, 1)$ a bounded lattice. A sub-universe S of $(L, \vee, \wedge)$ is a non-empty subset of L s.t. $\{0, 1\} \subseteq S$ and S is closed under the lattice operations.

If S is a sub-universe of $(L, \vee, \wedge, 0, 1)$, then $(S, \vee_{S^2}, \wedge_{S^2}, 0, 1)$ is a bounded sub-lattice of $(L, \vee, \wedge, 0, 1)$, and every bounded sub-lattice is obtained in this way. In other words, there is a bijection between $\mathcal{S}_L$, the set of bounded sub-lattices of $(L, \vee, \wedge, 0, 1)$, and $\mathcal{L}_L$, set of sub-universes of $(L, \vee, \wedge, 0, 1)$:

$$\begin{aligned} \mathcal{S}_L &\mapsto \mathcal{L}_L \\ S &\to \left(S, \vee_{S^2}, \wedge_{S^2}, 0, 1\right) \end{aligned} \qquad\qquad \begin{aligned} \mathcal{L}_L &\mapsto \mathcal{S}_L \\ (L', \vee', \wedge', 0', 1') &\mapsto L' \end{aligned}$$

Problem 44. If $(L, \vee, \wedge, 0, 1)$ a bounded lattice and S_1, S_2 sub-universes of $(L, \vee, \wedge, 0, 1)$, then $S_1 \cap S_2$ are sub-universes of $(L, \vee, \wedge, 0, 1)$.

Should be false but complete.

Definition 12. Let $(L, \vee, \wedge, 0, 1)$, $(L', \vee', \wedge', 0', 1')$ bounded lattices. A function $F : L \to L'$ is an homomorphism from the first to the latter lattice if, $\forall x, y \in L$:

1. $F(x \circ y) = F(x) \circ' F(y)$
2. $F(0) = 0'$
3. $F(1) = 1'$

Definition 13. Let $(L, \vee, \wedge, 0, 1), (L', \vee', \wedge', 0', 1')$ bounded lattices. A homomorphism $F : L \to L'$ is an isomorphism if it is bijective and its inverse is a homomorphism.

Theorem 19. *If F a bijective homomorphism between two bounded lattices, then F is an isomorphism.*

Proof 19. Since F is bijective its inverse is bijective, which means each element in L' corresponds to a unique element in L via F^{-1}.
Since $F(0) = 0', F(1) = 1'$, we have $F^{-1}(0') = 0$ and $F^{-1}(1') = 1$. Now let $v, w \in L'$. We wish to prove

$$F^{-1}(v \circ' w) = F^{-1}(v) \circ F^{-1}(w) \tag{2}$$

Observe that

$$F\left[F^{-1}(v) \circ F^{-1}(w)\right] = F\left[F^{-1}(v)\right] \circ' F\left[F^{-1}(w)\right] = v \circ' w$$

At the same time,

$$F\left[F^{-1}(v \circ' w)\right] = v \circ' w$$

In other words, both sides of equation (2) map to the same value via F. But since F is a bijection, two distinct elements can never map to the same value. Then the l.h.s. and the r.h.s. are equal. ■

Theorem 19 ensures that, when dealing with bounded lattices, all bijective homomorphisms are isomorphisms. This was also the case for simple lattices (**Theorem 12**). The reader may wonder why the definition of isomorphism isn't simply a bijective homomorphism.

The reason is that, though bijective homomorphisms are always isomorphisms in the case of simple and bounded lattices, there a structures where this doesn't hold. See **Chapter 3.3** on poset homomorphisms for an example of this.

We will write $F : ((L, \vee, \wedge, 0, 1) \to (L', \vee', \wedge', 0', 1')$ to denote a homomorphism from the first to the latter lattice. This should not be interpreted as saying that the domain of F is a subset of $(L, \vee, \wedge, 0, 1)$, which makes no sense.

Theorem 20. *If* $F : (L, \vee, \wedge, 0, 1) \to (L', \vee', \wedge', 0', 1')$ *is a homomorphism, then* I_F *is a sub-universe of* $(L', \vee', \wedge', 0', 1')$. *This means F is also a homomorphism from* $(L, \vee, \wedge, 0, 1)$ *to* $(I_F, \vee'_{I_F^2}, \wedge'_{I_F^2}, 0', 1')$.

Proof 20. We know $I_f \subseteq L'$, and since F is a homomorphism $\{0', 1'\} \in I_F$. In other words, I_F is non-empty. We must only show that I_F is closed. Given $y_0, y_1 \in I_F$, there are at least two values $x_0, x_1 \in L$ s.t. $F(x_0) = y_0, F(x_1) = y_1$. Then $y_0 \circ' y_1 = F(x_0) \circ' F(x_1) = F(x_0 \circ x_1) \in I_F$. ■

5.2 Congruences over bounded lattices

Naturally, it is possible to have congruence relations over a bounded lattice.

Definition 14. A congruence over $(L, \vee, \wedge, 0, 1)$ is an equivalence relation θ s.t. θ is a congruence over $(L, \vee, \wedge)$.

Recall that we defined $x/\theta \tilde{\circ} y/\theta = (x \circ y)/\theta$. The 5-uple $(L/\theta, \tilde{\vee}, \tilde{\wedge}, 0/\theta, 1/\theta)$ is called *the quotient* of $(L, \vee, \wedge, 0, 1)$ over θ and is denoted with $(L, \vee, \wedge, 0, 1)/\theta$.

Theorem 21. *Let* $(L, \vee, \wedge, 0, 1)$ *a bounded lattice and* θ *a congruence over* $(L, \vee, \wedge, 0, 1)$.

- $(L/\theta, \tilde{\vee}, \tilde{\wedge}, 0/\theta, 1/\theta)$ *is a bounded lattice.*
- π_θ *is a homomorphism from* $(L, \vee, \wedge, 0, 1)$ *to* $(L, \vee, \wedge, 0, 1)$ *and* $\ker(\pi_\theta) = \theta$.

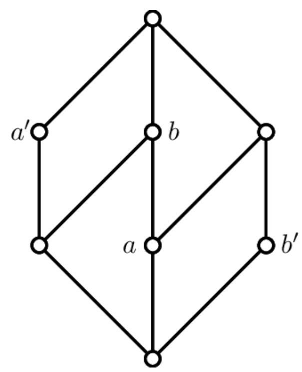
Proof 21. Analogous to the proof of **Theorem 18**.

5.3 Complemented lattices

Imagine any bounded lattice, and picture in particular the Hasse diagram associated to the lattice viewed as a poset. It is easy to conceive that some pair of elements may have no common ancestor other than 0, and no common successor other than 1. We call such elements *complements*.

Definition 15. Let $(L, \vee, \wedge, 0, 1)$ a bounded lattice. We say $a \in L$ is complemented if there is some $b \in L$ s.t. $a \vee b = 1, a \wedge b = 0$. Such b is called the complement of a.

The image below depicts a lattice and marks the complements as a and a', b and b'.



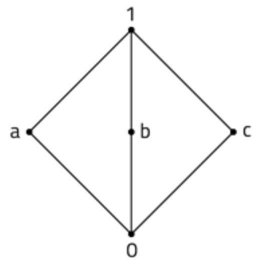
By definition, 0 is the common ancestor of all elements, and 1 the common successor of all elements. Inversely, all elements are predecessors of 1 and successors of 0. Thus, if 1 is a complement of some element a, this element must be 0, and vice-versa.

Given a bounded latice $(L, \vee, \wedge, 0, 1)$, we define $c : L \mapsto L$ as the unary *complement* operation. Instead of writing $c(x)$ we shall write x^c.

Definition 16. A complemented lattice is a 6-upla $(L, \vee, \wedge, {}^c, 0, 1)$ s.t. $(L, \vee, \wedge, 0, 1)$ is a bounded lattice and ^{c} is a unary operation over L s.t. $\forall x \in L : x \vee x^c = 1, x \wedge x^c = 0$.

Note that is is possbile to define more than one unary operation that satisfies the definition of complement.

Problem 45. Consider the diamond poset $(\{1, 2, 3, 5, 30\}, |)$. It clearly corresponds to bounded lattice in the algebraic sense. Find all unary operations λ s.t. $(L, \vee, \wedge, \lambda, 0, 1)$ is a complemented lattice.

> The image below depicts the diamond lattice, where the prime numbers take the positions of a, b, c.
>
> 
>
>
> Observe that a, b and c are all complements of each other. Thus, any λ s.t. $(L, \vee, \wedge, \lambda, 0, 1)$ is a complemented lattice must map each prime to either of the other two primes. Thus, if we let $\mathcal{P} = \{2, 3, 5\}$ the set of primes in the lattice, the set of all complement functions is
>
> $$\begin{aligned}\{\lambda : L \to L \mid \lambda(0) &= 1,\\ \lambda(1) &= 0,\\ \forall p \in \mathcal{P} : \exists p' \in \mathcal{P} : p \neq p' &\wedge \lambda(p) = p'\}\end{aligned}$$
>
> It is easy to observe that there are 2^3 such functions, since we have 2 options for each of the 3 prime numbers.

Let $(P, \leq)$ a poset with a maximum and minimum, and assume there is some unary operation $\lambda : P \to P$ s.t. $\sup\{x, \lambda(x)\} = 1, \inf\{x, \lambda(x)\} = 0$. Then defining $\vee$ and $\wedge$ as the sup and inf functions of the poset satisfies that $(L, \vee, \wedge, \lambda, 0, 1)$ is a complemented lattice.

Furthermore, by virtue of Dedekind's theorem, every complemented lattice is obtained in this way. This entails that a poset with maximum, minimum and a complement operation λ is, in a certain sense, the same than its corresponding complemented lattice.

5.4 Complemented sub-lattices

Definition 17. Given two complemented lattices $(L, \vee, \wedge, {}^c, 0, 1)$ and $(L', \vee', \wedge', {}^{c\prime}, 0', 1')$, we say the first is a complemented sub-lattice of the latter iff

- $L \subseteq L$
- $0 = 0', 1 = 1'$
- $\vee = \vee'_{|L^2}, \wedge = \wedge'_{|L^2}, {}^c = {}^c_{|L}$

Definition 18. Let $(L/\theta, \widetilde{\vee}, \widetilde{\wedge})$ a complemented lattice. A set $S \subseteq L$ is a sub-universe of the lattice if $\{0, 1\} \subseteq S$ and S is closed under $\wedge$, $\vee$ and ^{c}.

As in previous cases, if S is a sub-universe of $(L, \vee, \wedge, {}^c, 0, 1)$, then $(S, \vee_{|S^2}, \wedge_{|S^2}, {}^c_{|S^2}, 0, 1)$ is a complemented sub-lattice of $(L, \vee, \wedge, {}^c, 0, 1)$, and every complemented sub-lattice is obtained in this way. In other words, there is a bijection between the set of complemented sub-lattice of $(L, \vee, \wedge, {}^c, 0, 1)$ and the set of sub-universes of $(L, \vee, \wedge, {}^c, 0, 1)$.

5.5 Homorphisms of complemented lattices

Definition 19. Let $(L, \vee, \wedge, {}^c, 0, 1)$, $(L', \vee', \wedge', {}^{c\prime}, 0', 1')$ two complemented lattices. A function $F : L \mapsto L'$ is a homomorphism from the first to the latter if $\forall x, y \in L$:

- $F(x \circ y) = F(x) \circ' F(y)$.
- $F(x^c) = F(x)^{c'}$
- $F(0) = 0', F(1) = 1'$.

A homomorphism is an isomorphism if it is bijective and its inverse is a homorphism. In complemented sub-lattices, like all lattices so far, it suffices to show that a homomorphism is bijective to prove that it's an isomorphism.

Theorem 22. *If $F : (L, \vee, \wedge, {}^c, 0, 1) \mapsto (L', \vee', \wedge', {}^{c\prime}, 0', 1')$ is a bijective homomorphism, then it is an isomorphism.*

Proof 22. Analogous to previous cases.

Theorem 23. *If $F : (L, \vee, \wedge, {}^c, 0, 1) \mapsto (L', \vee', \wedge', {}^{c\prime}, 0', 1')$ is a homomorphism, then I_F is a sub-universe of $(L', \vee', \wedge', {}^{c\prime}, 0', 1')$. Which means F is also a homomorphism from $(L, \vee, \wedge, {}^c, 0, 1)$ to $(I_F, \vee'_{|I_F^2}, \wedge'_{|I_F^2}, {}^{c'}, 0', 1')$.*

Proof 23. Analogous to previous cases.

5.6 Congruences over complemented lattices

Definition 20. A congruence over $(L, \vee, \wedge, {}^c, 0, 1)$ is an equivalence relation θ s.t. θ is a congruence over $(L, \vee, \wedge, 0, 1)$ and $x/\theta = y/\theta \Rightarrow x^c/\theta = y^c/\theta$.

These conditions allow us to define $\widetilde{\vee}$ and $\widetilde{\wedge}$ in a fashion analogous to previous cases:

$$x/\theta \,\widetilde{\circ}\, y/\theta = (x \circ y)/\theta$$
$$(x/\theta)^{\widetilde{c}} = x^c/\theta$$

The 6-uple $(L/\theta, \widetilde{\vee}, \widetilde{\wedge}, {}^{\widetilde{c}}, 0/\theta, 1/\theta)$ is called the *quotient space* of $(L, \vee, \wedge, {}^c, 0, 1)$ over θ and we denote it as $(L, \vee, \wedge, {}^c, 0, 1)/\theta$.

Theorem 24. *If $(L, \vee, \wedge, {}^c, 0, 1)$ a complemented lattice and θ a congruence over $(L, \vee, \wedge, {}^c, 0, 1)$:*

- $(L/\theta, \widetilde{\vee}, \widetilde{\wedge}, {}^{\widetilde{c}}, 0/\theta, 1/\theta)$ *is a complemented lattice.*
- π_θ *is a homomorphism from* $(L, \vee, \wedge, {}^c, 0, 1)$ *to* $(L/\theta, \widetilde{\vee}, \widetilde{\wedge}, {}^{\widetilde{c}}, 0/\theta, 1/\theta)$ *and* $\ker(\pi_\theta) = \theta$.

Proof 24. (1) A previous theorem ensures that $(L/\theta, \widetilde{\vee}, \widetilde{\wedge}, 0/\theta, 1/\theta)$ is a bounded lattice, so we only to verify that the lattice identities hold for the ${}^{\widetilde{c}}$ operation.
Let $x/\theta \in L/\theta$. By assumption $x \circ x^c = 1$, which entails $(x \circ x^c)/\theta = 1/\theta$. Then, by definition,

$$x/\theta \widetilde{\circ} (x^c)/\theta = 1/\theta$$
$$\iff x/\theta \widetilde{\circ} (x/\theta)^{\widetilde{c}} = 1/\theta$$

(2) A previous theorem ensures that π_θ is a homorphism from $(L, \vee, \wedge, 0, 1)$ to $(L/\theta, \widetilde{\vee}, \widetilde{\wedge}, 0/\theta, 1/\theta)$ whose kernel is θ. We must only ensure that it satisfies the homorphism definition for the complement operation.
Let $x \in L$. We wish to prove $\pi_\theta(x^c) = \pi_\theta(x)^{\widetilde{c}}$. By definition,

$$\pi_\theta(x)^{\widetilde{c}} = (x/\theta)^{\widetilde{c}} = (x^c)/\theta = \pi_\theta(x^c) \blacksquare$$

Theorem 25. *If $F : (L, \vee, \wedge, {}^c, 0, 1) \mapsto (L', \vee', \wedge', {}^{c'}, 0', 1')$ is a complemented lattice homomorphism, then $\ker(F)$ is a congruence over $(L, \vee, \wedge, {}^c, 0, 1)$.*

This is the analogue to **Theorem 17**, which stated this was the case for general lattices.

Proof 25. Let $\lambda = \ker(F)$. By definition, λ is a congruence over $(L, \vee, \wedge, 0, 1)$. Then all that remains to be shown is that $x/\lambda = y/\lambda \Rightarrow x^c/\lambda = y^c/\lambda$.

Let $x, y \in L$ s.t. $x/\lambda = y/\lambda$. This entails $F(x) = F(y)$. Since F a homomorphism, $F(x^c) = F(x)^c$, which entails

$$F(x)^c = F(y)^c \Rightarrow F(x^c) = F(y^c) \Rightarrow (x^c, y^c) \in \ker(F)$$

It follows directly that $x^c/\lambda = y^c/\lambda$. ■

5.7 A notational convention

In the n-uples we have studied (posets and lattices of various kinds), the first element of the n-uple was called its *universe*. We shall use bold letters to denote the universes of these structures. Thus, the phrase "$\mathbf{L}$ is a bounded lattice" equates to saying $(L, \vee, \wedge, 0, 1)$ is a bounded lattice.

Then writing that $F : \mathbf{L} \mapsto L'$ is a homomorphism equates to saying $F : (L, \vee, \wedge, 0, 1) \mapsto (L', \vee', \wedge', 0', 1')$ is a homomorphism. Similarly, writing $\mathbf{L}/\theta$, where θ a congruence, will equate to writing the quotient space of whatever n-uple is signified by $\mathbf{L}$.

6 Boolean algebras

We have so far studied several kinds of mathematical structures separately. In particular, we have studied different kinds of lattices, observing a special property which defined them.

Now, we come to the study of structures which exhibit several of these properties simultaneously. In particular, we will develop an understanding of bounded and distributive lattices, show the connection of this combination with complemented lattices, and from there develop the concept of a Boolean algebra.

Definition 21. A bounded or complemented lattice **L** is said to be distributive when $(L, \vee, \wedge)$ is distributive.

Let Dis_1 denote distributivity of $\wedge$ with respect to $\vee$, and Dis_2 the converse.

Theorem 26. *Let* $(L, \vee, \wedge)$ *a lattice. Then* $(L, \vee, \wedge)$ *satisfies* Dis_1 *iff it satisfies* Dis_2.

Proof 26. Assume $(L, \vee, \wedge)$ satisfies Dis_1. Let $a, b, c \in L$ fixed. Then

$$(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c)$$

Commutativity then gives

$$((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = (a \wedge (a \vee b)) \vee (c \wedge (a \vee b))$$

A funamental property of lattices is that $a \wedge (a \vee b) = a$. Using this property with Dis_1,

$$(a \wedge (a \vee b)) \vee (c \wedge (a \vee b)) = a \vee ((c \wedge a) \vee (c \wedge b))$$

Due to the associative property,

$$= a \vee ((c \wedge a) \vee (c \wedge b)) = (a \vee (c \wedge a)) \vee (c \wedge b)$$

Commutativity gives

$$(a \vee (c \wedge a)) \vee (c \wedge b) = (a \vee (a \wedge c)) \vee (b \wedge c) = a \vee (b \wedge c)$$

Then we have proven $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. ■.
The other direction of the double implication is analogous.

Definition 22. A Boolean algebra is a complemented lattice **L** that is distributive.

Theorem 27. *Let* **L** *a bounded lattice that is distributive. Then every element has at most one complement.*

Proof 27. Let $x, y, z \in L$ fixed. Assume $x \vee y = x \vee z = 1$ and $x \wedge y = x \wedge z = 0$. Observe that $y = y \wedge 1 = y \wedge (x \vee z)$. Because **L** is distributive, we have $y = (y \wedge x) \vee (y \wedge z)$. Then $y = 0 \vee (y \wedge z) = y \wedge z$.

The same line of reasoning gives $z = z \wedge 1 = z \wedge (x \vee y)$, from which follows $z = (z \wedge x) \vee (z \wedge y) = z \wedge y$.

$\therefore z = z \wedge y = y \wedge z = y$.

$\therefore z = y$.

Theorem 28. *Let* $(B, \vee, \wedge, {}^c, 0, 1)$ *a Boolean algebra. For any* $x, y \in B$, $y = (y \wedge x) \vee (y \wedge x^c)$.

Proof 28. Let $x, y \in B$. Then

$$\begin{aligned}
(y \wedge x) \vee (y \wedge x^c) &= [(y \wedge x) \vee y] \wedge [(y \wedge x) \vee x^c] && \{\text{Dist.}\} \\
&= [(y \vee y) \wedge (y \vee x)] \wedge [(y \vee x^c) \wedge (x \vee x^c)] && \{\text{Dist.}\} \\
&= [y \wedge (y \vee x)] \wedge [(y \vee x^c) \wedge 1] && \{\text{Comp., abs.}\} \\
&= y \wedge (y \vee x^c) \\
&= y
\end{aligned}$$

where the last two steps use the property $y \wedge (y \vee x) = y$.

Theorem 29. *Let* ***B*** *a Boolean algebra and* $x, y \in B$. *Then:*

- $(x \wedge y)^c = x^c \vee y^c$ *(DeMorgan's law 1)*
- $(x \vee y)^c = x^c \wedge y^c$ *(DeMorgan's law 2)*
- $(x^c)^c = x$
- $x \wedge y = 0 \iff y \leq x^c$
- $x \leq y \iff y^c \leq x^c$

If one thinks of the associated posset, the proposition $x \wedge y = 0$ may be read as "y is not an ancestor of x". Thus, the fourth property states if y is not an ancestor of x, then it must be an ancestor of x^c.

Similarly, the last property states that if x is an ancestor of y, y^c is an ancestor of x^c.

Proof 29. We will prove the fourth and fifth properties.

(Property 4) Assume $x \wedge y = 0$. The previous theorem gives

$$\begin{aligned}
y &= (y \wedge x) \vee (y \wedge x^c) \\
&= y \wedge x^c
\end{aligned}$$

$\therefore y \leq x^c$.

Now assume $y \leq x^c$. Then $y \wedge x \leq x^c \wedge x$.

$\therefore y \wedge x \leq 0$.

$\therefore y \wedge x = 0$.

(Property 5) Assume $x \leq y$. Then $(x \wedge y) = x$. Then $(x \wedge y)^c = x^c$, and $x^c \vee y^c = x^c$. Then $x^c \wedge y^c = y^c$ and $y^c \leq x^c$.

Now assume $y^c \leq x^c$. Then $(y^c \wedge x^c) = y^c$. Then $(y^c)^c \vee (x^c)^c = (y^c)^c$, which entails $y \vee x = y$. Then $x \leq y$.

■

Problem 46. Due the properties of the previous theorem hold for any complemented lattice?

The answer is no; we need distributivity. But prove it. Complete.

6.1 Prime filters and Rasiova-Sikorski's theorem

Definition 23. A filter of a lattice $(L, \vee, \wedge)$ will be any non-empty subset $F \subseteq L$ s.t.

- $x, y \in F \Rightarrow x \wedge y \in F$
- $x \in F$ and $x \leq y \in F$

Problem 47. Describe the filters of $(\mathbb{R}, \max, \min)$. For any given filter, does it always contain an infimum?

Observe that $(\mathbb{R}, \max, \min)$ induces via Dedekind's theorem the totally ordered set $(\mathbb{R}, \leq)$, where $\leq$ is the usual order. Consider any filter $F \subseteq \mathbb{R}$. The inclusion of any element in F implies the inclusion of all numbers greater than that element. Thus, the filters of $(\mathbb{R}, \max, \min)$ consists of all continuous subsets of $\mathbb{R}$; i.e.

$$\text{Set of filters of } (\mathbb{R}, \max, \min) = \{[x, \infty) : x \in \mathbb{R}\}$$

Clearly, since any filter is of the form $[x, \infty)$ with $x \in \mathbb{R}$, x is always the infimum of that filter.

Problem 48. Find all filters of $(\{1, 2, 3, 6, 12\}, \mathrm{lcm}, \gcd)$.

Evidently, $\{1, 2, 3, 6, 12\}$ is a filter, and is the only filter which contains 1.

Consider a filter which contains 2. If it contains 3 it must contain 1 and we are back in the first case. So $\{2, 6, 12\}$ is a filter. A similar argument leads to $\{3, 6, 12\}$.

Lastly, $\{6, 12\}$ and $\{12\}$ are filters.

Let us present some notation. Given $S \subseteq L$, we use $[S)$ to denote the set

$$\{x \in L : y \geq (s_1 \wedge \ldots \wedge s_n) \text{ for some } s_1, \ldots, s_n \in S, n \geq 1\}$$

and we call it the filter *generated* by S.

The set $[S)$ is clearly a subset of L. If $l \in L$ is a successor of any element of S, or of the infimum between any set of elements in S, then $l \in [S)$. In a certain sense, the elements of $[S)$ are the successors of all elements of S or some of their predecessors.

Since any element in S is a successor to itself, all elements of S are in $[S)$. In other words, $S \subseteq [S) \subseteq L$.

When S is finite, $[S) = \{y \in L : y \geq \inf(S)\}$. When S is infinite but has an infimum, in many cases the statement will hold as well, but there are exceptions.

Example 1. Let $\mathbf{L} = (\mathcal{P}(\mathbb{N}), \cup, \cap)$ and $S = \{\mathbb{N} - n : n \in \mathbb{N}\}$. The infimum of S is $\emptyset$ and $[S) = \{A \in \mathcal{P}(\mathbb{N}) : \mathbb{N} - A \text{ is finite}\}$.

Then it doesn't hold that $[S) = \{y \in L : y \geq \inf S\}$.

Theorem 30. *Assume S is non-empty. Then $[S)$ is a filter. Furthermore, if F a filter and $S \subseteq F$, then $[S) \subseteq F$. In other words, $[S)$ is the minimal filter which contains S.*

Proof 30. Since $S \subseteq [S)$ we have $[S) \neq \emptyset$. It is trivial to observe that $[S)$ satisfies that if an element is in $[S)$, all its successors will also be in $[S)$. Let us show that the infimum of any pair in $[S)$ is also in $[S)$.

Assume $x, y \in [S)$. Then $x \geq s_1 \wedge \ldots \wedge s_n$ and $y \geq t_1 \wedge \ldots \wedge t_m$ for $n, m \geq 1$ and $s_j, t_j \in S$. Then

$$x \wedge y \geq (s_1 \wedge \ldots \wedge s_n) \wedge (t_1 \wedge \ldots t_m)$$

which completes the proof.

Definition 24. Let $(P, \leq)$ a poset. A subset $C \subseteq P$ is a chain if for every $x, in \in C, x \leq y$ or $y \leq x$.

Chains may be infinite and given an infinite chain C, there may not exist an infinite sequence $\{c_1, c_2, \ldots\}$ s.t. $C = \{c_n : n \in \mathbb{N}\}$.

Example 2. Every subset of $\mathbb{R}$ is a chain of $(\mathbb{R}, \leq)$. Observe that there is no discrete infinite sequence $c_1, c_2, \ldots$ which may account for a subset of $\mathbb{R}$.

Theorem 31 (Zorn's theorem)**.** *Let $(P, \leq)$ a poset and assume every chain of $(P, \leq)$ has an upper bound. Then there is a maximal element in $(P, \leq)$.*

Proof 31. Complete.

Definition 25 (Prime filter)**.** A filter F on a lattice $(L, \vee, \wedge)$ is called *prime* when $F \neq L$ and $x \vee y \in F \Rightarrow x \in F \vee y \in F$.

Problem 49. Show that every filter of $(\mathbb{R}, \max, \min)$ other than $\mathbb{R}$ is prime.

The lattice $\mathbf{L} = (\mathbb{R}, \max, \min)$ induces the total order $(\mathbb{R}, \leq)$. Let $\mathcal{F}$ an arbitrary filter of $\mathbf{L}$ different from $\mathbb{R}$. Assume $x \max y \in \mathcal{F}$ for $x, y \in \mathbb{R}$. Since $x \max y \in \{x, y\}$, either $x \in \mathcal{F}$ or $y \in \mathcal{F}$. Then $\mathcal{F}$ is prime. ■

Problem 50. Find all prime filters over $\mathbf{L} = (\{1, 2, 3, 6, 12\}, \mathrm{lcm}, \gcd)$.

In **Problem 48** we found all filters of $\mathbf{L}$. The question is which, except for L, were prime?

Clearly, $\{6, 12\}$ is not prime, because $6 = 3 \vee 2$ and it doesn't contain either 3 nor 2. Same observation yields that $\{2, 6, 12\}$ and $\{3, 6, 12\}$ are prime. Finally, $\{12\}$ is trivially prime: $12 \vee 12 = 12$.

Theorem 32 (Prime filter theorem)**.** *Let $\mathbf{L}$ a distributive lattice and F a filter of $\mathbf{L}$. Assume $x_0 \in L - F$. Then there is a prime filter P s.t. $x_0 \notin P$ and $F \subseteq P$.*

Proof 32. Let

$$\mathcal{F} := \{F_1 : F_1 \text{ is a filter}, x_0 \notin F_1, F \subseteq F_1\}$$

Since $F \in \mathcal{F}, \mathcal{F} \neq \emptyset$ and $\mathbf{F} = (\mathcal{F}, \subseteq)$ is a poset. Let us prove that every chain in the poset has an upper bound.

Let C a chain over $\mathbf{F}$. If $C = \emptyset$, every element in $\mathcal{F}$ is an upper bound. If $C \neq \emptyset$, we can define

$$G = \{x \in L : x \in F_1 \text{ for some } F_1 \in C\}$$

It is clear that $G \neq \emptyset$. Assume $x, y \in G$. Let $F_1, F_2 \in \mathcal{F}$ s.t. $x \in F_1$ and $y \in F_2$.

If $F_1 \subseteq F_2$, since F_2 a filter we have $x \wedge y \in F_2 \subseteq G$. If $F_2 \subseteq F_1$ then $x \wedge y \in F_1 \subseteq G$. Since C a chain $x \wedge y \in G$. The remaining property is proved in analogous fashion.

$\therefore G$ is a filter.

Since $x_0 \notin G$ we know $G \in \mathcal{F}$ is upper-bound of C. Due to Zorn's theorem, $(\mathcal{F}, \subseteq)$ has a maximal element $\mathcal{M}$. We shall show $\mathcal{M}$ is prime.

Assume $x \vee y \in \mathcal{M}$ and $x, y \notin \mathcal{M}$. Observe that $[\mathcal{M} \cup \{x\})$ is a filter which properly contains $\mathcal{M}$. Since $\mathcal{M}$ is maximal of $(\mathcal{F}, \subseteq)$ we have $x_0 \in [\mathcal{M} \cup \{x\})$. Analogously, $x_0 \in [\mathcal{M} \cup \{y\})$.

Since $x_0 \in [\mathcal{M} \cup \{x\})$ there are $m_1, \ldots, m_n \in \mathcal{M}$ s.t.

$$x_0 \geq m_1 \wedge \ldots \wedge m_n \wedge x$$

Since $x_0 \in [\mathcal{M}, \{y\})$ there are $m'_1, \ldots, m'_r \in \mathcal{M}$ s.t.

$$x_0 \geq m'_1 \wedge \ldots m'_r \wedge y$$

Let $m := m_1 \wedge \ldots \wedge m_n \wedge m'_1 \wedge \ldots \wedge m'_r$. Then we have $x_0 \geq m \wedge x$ and $x_0 \geq m \wedge y$.

$\therefore x_0 \geq (m \wedge x) \vee (m \wedge y) = m \wedge (x \vee y)$.

But this is absurd because $x_0 \notin \mathcal{M}$. The contradiction ensued from assuming $x, y \notin \mathcal{M}$.

$\therefore$ Either $x \in \mathcal{M}$ or $y \in \mathcal{M}$.

$\therefore$ $\mathcal{M}$ is prime.

Let us unpack the theorem. Assume **L** is a distributive lattice and F is a filter over it. Assume as well that some $x_0 \in L$ is not contained in the filter. We are interested in the family $\mathcal{F}$ of filters which do not contain x_0 and contain all elements of F. Informally, we may call these *extensions of* F *around* x_0. Such family conforms a poset $(\mathcal{F}, \subseteq)$. The theorem states that *(1)* this poset has a maximal element and *(2)* it is a prime filter.

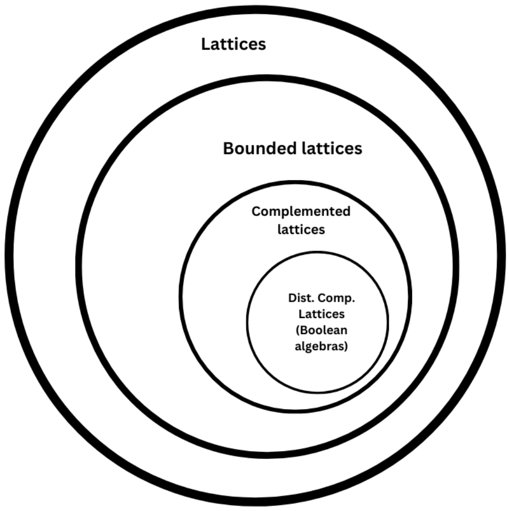
Theorem 33 (Rasiova-Sikorski's)**.** *Let* $\boldsymbol{B}$ *a Boolean algebra. Let* $\varphi \in B$ *a non-zero element. Assume* $(A_1, A_2, \ldots)$ *is an infinituple of subsets of* B *s.t. each subset has an infimum. Then there is a prime filter* P *which satisfies:*

- $\varphi \in P$
- $\forall j \in \mathbb{N} : A_j \subseteq P \Rightarrow inf(A_j) \in P$

Proof 33. It is accepted without proof.

7 Structures and their associated languages

We have so far studied several kinds of structures. We begain with posets and noted that they were, in a certain sense, equivalent to algebraic lattices. We studied different families of lattices, which are schematized in the diagram below.



We will associate to each structure a set of sentences which we call *elementary formulas*. These formulas will serve as axioms to, in turn, conform another type of sentence termed *elementary proofs*. It is important to observe that these sentences are relative to the particular kind of structure that is being considered.

Elementary formulas will be formed with the usual symbols $\forall, \exists, \neg, \wedge, \ldots$ etc. We use $x, y, z, \ldots$ to denote variables and $a, b, c, \ldots$ to denote fixed elements. For instance,

$$\neg\exists y\,(x \leq y \wedge \neg(y = x))$$

is an elementary formula. Importantly, if φ is a formula, then the type of φ is **word**.

A formula will be true or false depending on a particular poset $(P, \leq)$. The variables of the formula will receive their values from said poset. When the formula has no free variables, we say it is an *elementary poset sentence*. Furthermore, as a convention, the quantifiers $\forall$ and $\exists$ always range over P. To keep matters clear, we will never quantify over fixed elements; i.e. $\forall a(a = x)$ is not an elementary formula.

Example 3. Let $\mathbf{P} = (\mathbb{N}, |)$. The formula $(x \leq y)$ is true when x is assigned 6 and y 36. But the formula $\forall x \forall y\ (x \leq y \vee yx)$ is false.

7.1 Free variables