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

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 $R = \left\{(x, y) \in \mathbb{R}^2 : x = y\right\}$ 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 $R = \left\{(x, y) \in A^2 : x = y\right\}$.*

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

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

always with z elements.

Problem 6 *Let $R = \left\{(x, y) \in \mathbb{N}^2 : x, y \leq 6\right\} \cup \left\{(x, y) \in \mathbb{N}^2 : x > 6 \wedge y > 6\right\}$. 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 $|\{i/R : i \in A\}| = 5$.

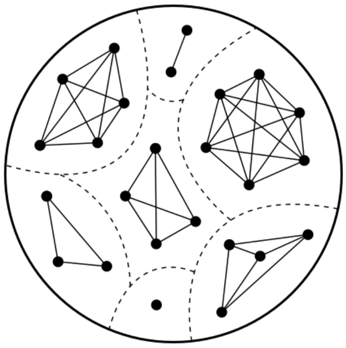
> False. It depends on R, which is unspecified. E.g. we have shown that if $R = A^2$ then $|A/R| = 1$.

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

> False, but it is made look like it is true. By definition of $R = \left\{(x,y) \in A^2 : x = y\right\}$ we have $x, y \in A \wedge x \neq y \Rightarrow \neg(xRy)$. So $a \in A$ belongs to a single equivalence 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 $C \in A/R$.

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



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 $A/R = \{\{1, 2, 3\}\} \not\supseteq C$.

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

(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 $R = \left\{(a, b) \in A^2 : a = b\right\}$.

$(\Leftarrow)$ Assume $R = \left\{(a, b) \in A^2 : a = b\right\}$. 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.

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 *at least* contains 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*

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

are bijections one the inverse of the other.

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 $R \ddot{\propto} A$, 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 $R \ddot{\propto} A$ 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

In general, defining $f : A/R \mapsto B$ leads to ambiguity. 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.** *(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.*

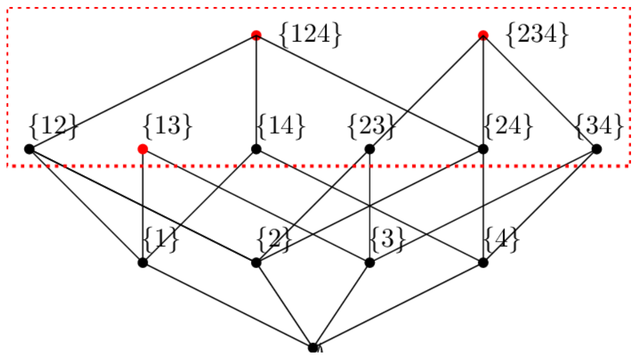
> **Proof.** Assume $(P, \leq)$ is a poset with two distinct maximums x, y. By definition then $x \leq y$ and $y \leq x$. By anti-symmetry we have $x = y$, which is a contradiction.

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 $m_j \not\leq m_i$) 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,

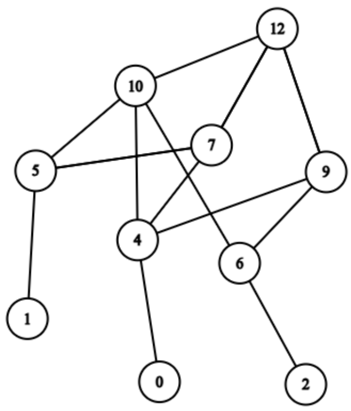
$$\{a \in P : a \text{ is upper bound of } \emptyset \text{ in } (P, \leq)\} = P$$

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

(3) The statement is false. The hypothesis gives $P \neq \emptyset$, and we know any $a \in P$ is an upper-bound of $\emptyset$. If we assume $\emptyset$ has a supremum over $(P, \leq)$, then it is the least upper-bound. In other words, it is some $m \in P$ s.t. $m \leq a$ for any $a \in P$. By definition, m is a minimum.

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 $x_i \not\leq x_j$ 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 $\left\{x_i, x_j\right\}$ 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 $a \nleq u$. Then a is the least upper bound of P. $\blacksquare$

($\Leftarrow$) 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* $(P, \leq)$*?*

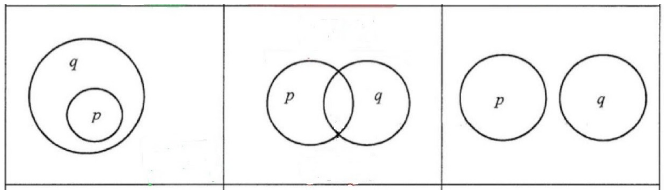
The order is the usual order, but over $P = \{0\} \cup (1, 2]$. The set S (and in fact P as well) has only one lower bound over $(P, \leq)$; namely, 0. Observe that 1 is not a lower bound because $1 \notin P$, and there is no such thing as the "first rational number". Since 0 is the *only* lower bound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

Problem 20 *Say true or false. Let*

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

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

$\mathcal{D}\left((x_0, y_0), r\right)$ 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 $F^{-1}(1) = 1, F^{-1}(2) = 2, 1 \nleq 2$.

The following theorem states that a homomorphism 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 $F(x) \prec' F(y)$.*

> **Problem 21** *Prove that if $(P, \leq), (Q, \leq')$ posets with an isomorphism F, then for all $x, y \in P$ we have $x \prec y \iff F(x) \prec' F(y)$.*
>
> $(\Rightarrow)$ Assume $x \prec y$. 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 $F(x) \prec' F(y)$.
>
> $(\Leftarrow)$ Assume $F(x) \prec' F(y)$. Then we have $x \leq y$ (because F^{-1} is an homomorphism). If $x = y$ and $F(x) \prec' F(y)$, we have $F(y)$ covers $F(x)$ but y does not cover x $(\perp)$. Then $x \prec y$.

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. $x \nleq m$. 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 $f : A^2 \longrightarrow A$ s.t. $\mathcal{D}_f = A$. 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,* $x \leq y \iff x \wedge y = x$*.*

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)* $x \wedge (x \vee y) = x$*.*

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

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. *(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. *(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 s.t.* $sup\,\{x, y\} = x \vee y$, $inf\,\{x, y\} = x \wedge y$, *for any* $x, y \in L$.

We call $\leq$ the order associated to $(L, \vee, \wedge)$ and $(L, \leq)$ the poset associated to $(L, \vee, \wedge)$.

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 $\wedge$).

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

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

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 $(S, \vee \mid_{S \times S}, \wedge \mid_{S \times S})$ 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.

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.*

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 $(I_F, \vee' |_{I_F \times I_F}, \wedge' |_{I_F \times I_F})$.*

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 $(L', \leq')$.*

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 allows us to define two binary operations $\hat{\vee}$, $\hat{\wedge}$ over L/θ as follows:

$$x/\theta \widetilde{\vee} y/\theta = (x \vee y)/\theta$$
$$x/\theta \widetilde{\wedge} y/\theta = (x \wedge y)/\theta$$

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

$$\left.\begin{matrix} 1\ \theta\ 2 \\ 4\ \theta\ 5 \end{matrix}\right\} \Rightarrow (1 \max 4)\theta(2 \max 5)$$

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

$(1 \max 4)/\theta = 4/\theta = \{4, 5\}$. In a sense, we are taking the supremum and infimum operations to a broader dimension, not applying to individual elements but to sets of equivalent elements.

Note. Observe that a congruence is an equivalence relation that is preserved in the supremum and infimum operations of a lattice. In the previous example, because it is a congruence, we expect that because 1 is equivalent to 2, and 4 is equivalent to 5, that the supremum of 1 and 4 matches the supremum of 2 and 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 $(L/\theta, \widetilde{\vee}, \widetilde{\wedge})$.

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 $x, y \in L$.

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