CHAPTER 2

ORDERED SETS

In this chapter we study binary relations which will be used extensively in the remainder of the book.

Ordered sets play a fundamental role, similar to the role of metric spaces, because they allow the *comparison* of two or more objects. Ordered sets will be used in most of the subsequent chapters (Chapter 3, Chapter 4, Chapter 9, etc.).

We define order relations and ordered sets, mappings between ordered sets and special elements such as minimal and maximal elements, upper and lower bounds. We study well-founded sets which form the general framework in which we can use proofs by induction. Finally, we study complete sets and monotone functions on complete sets, which form the basis of the semantics of programming languages.

The following book is very complete and at the same time quite readable: Garrett Birkhoff, *Lattice theory*, AMS, 3rd edition, Rhode Island (1979).

2.1 Order and preorder relations

2.1.1 Orders and strict orders

Definition 2.1 *An order relation or ordering is a reflexive, antisymmetric and transitive relation. A strict ordering is an irreflexive and transitive relation.*

REMARK 2.2
1. If $\mathcal{R}$ is a strict ordering on a set E, then the relation $\mathcal{R} \cup Id_E$ is an ordering on E. Conversely, if $\mathcal{R}'$ is an ordering, $\mathcal{R}' \setminus Id_E$ is a strict ordering.
2. If $\mathcal{R}$ is an antisymmetric and transitive relation, then the relation $\mathcal{R} \cup Id_E$ is an ordering and the relation $\mathcal{R} \setminus Id_E$ is a strict ordering.

Orderings are usually denoted by $\leq$, and strict orderings are denoted by $<$. By the preceding remark, it is easy to derive an ordering from the corresponding strict ordering and the converse, i.e.

- $x \leq y$ is equivalent to $x < y$ or $x = y$,
- $x < y$ is equivalent to $x \leq y$ and $x \neq y$.

2.1.2 Total orderings and partial orderings

If ordering $\mathcal{R}$ verifies $\forall e, e' \in E,\ e \neq e' \quad \Longrightarrow \quad \Big(e\ \mathcal{R}\ e' \text{ or } e'\ \mathcal{R}\ e\Big)$, then $\mathcal{R}$ is called a *total ordering*. Otherwise $\mathcal{R}$ is called a *partial ordering*.

Example 2.3
(i) The usual ordering on real numbers is a total ordering.
(ii) The divisibility relation on integers is a partial ordering ($a \leq_{\text{div}} b$ if and only if there exists c such that $b = ac$).
(iii) Inclusion on $\mathcal{P}(E)$ is a partial ordering if $|E| > 1$ and a total ordering if $|E| \leq 1$.

In the next example, we define common orderings on the free monoid A^* (see Definition 1.15).

Example 2.4
(i) The *prefix* ordering is a partial ordering on the monoid A^* that is defined as follows. String $u = u_1 \dots u_n$ is a prefix of string $v = v_1 \dots v_m$ if $n \leq m$ and $\forall i \leq n, u_i = v_i$.
(ii) We assume that alphabet A has a total ordering $\leq$. The *lexicographic* ordering $\preceq$ is a total ordering on the monoid A^* that is defined as follows. Let $u = u_1 \dots u_n$ and $v = v_1 \dots v_m$ be two strings. $u \prec v$ if

- either u is a prefix of v,
- or u and v coincide up to letter k, $u_{k+1} \neq v_{k+1}$ and $u_{k+1} \leq v_{k+1}$, with $0 \leq k < \inf(n, m)$.

2.1.3 Preorders

Definition 2.5 *A preorder relation is a transitive relation.*

Example 2.6 Let $E = \mathcal{P}_f(\mathbb{N})$ be the set of finite subsets of $\mathbb{N}$. Each subset X contains a least element, denoted by $\inf(X)$, and a greatest element, denoted by $\sup(X)$. We define the relation $\mathcal{R}$ on E by: $X\ \mathcal{R}\ X'$ if and only if $\inf(X) \leq \inf(X')$ and $\sup(X) \leq \sup(X')$. It is easy to see that this relation is transitive and reflexive. But it is not antisymmetric because $\big(X\ \mathcal{R}\ X'$ and $X'\ \mathcal{R}\ X\big)$ implies $\inf(X) = \inf(X')$ and $\sup(X) = \sup(X')$, but not necessarily $X = X'$.

Proposition 2.7 *If $\mathcal{R}$ is a preorder relation on E then $Id_E \cup (\mathcal{R} \cap \mathcal{R}^{-1})$ is an equivalence relation.*

Note that the relation $\equiv_{\mathcal{R}} = Id_E \cup (\mathcal{R} \cap \mathcal{R}^{-1})$ can be translated by $e \equiv_{\mathcal{R}} e'$ if and only if either $e = e'$ or $\big(e \mathrel{\mathcal{R}} e'$ and $e' \mathrel{\mathcal{R}} e\big)$.

Proof. The relation $Id_E \cup (\mathcal{R} \cap \mathcal{R}^{-1})$ is obviously reflexive and symmetric. We show that it is transitive, i.e. that

$$(Id_E \cup (\mathcal{R} \cap \mathcal{R}^{-1}))^2 \subseteq Id_E \cup (\mathcal{R} \cap \mathcal{R}^{-1}).$$

We see that $(Id_E \cup (\mathcal{R} \cap \mathcal{R}^{-1}))^2$ is equal to $Id_E \cup (\mathcal{R} \cap \mathcal{R}^{-1}) \cup (\mathcal{R} \cap \mathcal{R}^{-1})^2$. Because $\mathcal{R} \cap \mathcal{R}'$ is the intersection of two transitive relations, it is also transitive (see Exercise 3.5) and thus $(\mathcal{R} \cap \mathcal{R}^{-1})^2 \subseteq (\mathcal{R} \cap \mathcal{R}^{-1})$. □

Example 2.8 If we consider the preorder $\mathcal{R}$ of Example 2.6, the equivalence relation defined in Proposition 2.7 is

$$X \ \big(Id_E \cup (\mathcal{R} \cap \mathcal{R}^{-1})\big) \ X'$$

if and only if $\inf(X) = \inf(X')$ and $\sup(X) = \sup(X')$.

Let $\mathcal{R}$ be a preorder relation on E and let $\mathcal{E}$ be the associated equivalence. On the factor set $E/\ \mathcal{E}$ of E by $\mathcal{E}$, we can define the relation $\mathcal{R}'$ by $[e]_{\mathcal{E}} \mathrel{\mathcal{R}'} [e']_{\mathcal{E}}$ if and only if $e \mathrel{\mathcal{R}} e'$. This definition does not depend on the choice of the elements e and e' within their equivalence class, because if $e \mathrel{\mathcal{E}} e_1$ and $e' \mathrel{\mathcal{E}} e'_1$, then $e \mathrel{\mathcal{R}} e'$ if and only if $e_1 \mathrel{\mathcal{R}} e'_1$.

Exercise 2.1 Prove that $\mathcal{R}'$ does not depend on the choice of the elements e and e' within their equivalence class. ♢

Proposition 2.9 *The relation $\mathcal{R}'$ is antisymmetric and transitive; $\mathcal{R}'$ is an ordering if $\mathcal{R}$ is reflexive and $\mathcal{R}'$ is a strict ordering if $\mathcal{R}$ is irreflexive.*

Proof. $\mathcal{R}'$ is transitive, because $[e]_{\mathcal{E}} \mathrel{\mathcal{R}'} [e']_{\mathcal{E}}$ and $[e']_{\mathcal{E}} \mathrel{\mathcal{R}'} [e'']_{\mathcal{E}}$ imply $e \mathrel{\mathcal{R}} e'$ and $e' \mathrel{\mathcal{R}} e''$, and hence $e \mathrel{\mathcal{R}} e''$. It is antisymmetric because $\big([e]_{\mathcal{E}} \mathrel{\mathcal{R}'} [e']_{\mathcal{E}}$ and $[e']_{\mathcal{E}} \mathrel{\mathcal{R}'} [e]_{\mathcal{E}}\big)$ implies $\big(e \mathrel{\mathcal{R}} e'$ and $e' \mathrel{\mathcal{R}} e\big)$. Thus $(e, e') \in (\mathcal{R} \cap \mathcal{R}^{-1}) \subseteq \mathcal{E}$, and hence $[e]_{\mathcal{E}} = [e']_{\mathcal{E}}$.

$\mathcal{R}'$ is reflexive (resp. irreflexive) if $\mathcal{R}$ is reflexive (resp. irreflexive). □

This ordering $\mathcal{R}'$ will be called the *factor ordering* of the preorder $\mathcal{R}$.

Example 2.10 Again with the preorder of Example 2.6, the factor set of $E = \mathcal{P}_f(\mathbb{N})$ can be identified with the set of pairs (a, b) of integers such that $a \leq b$. On this set the ordering $\mathcal{R}'$ is defined by $(a, b) \mathrel{\mathcal{R}'} (a', b')$ if and only if $a \leq a'$ and $b \leq b'$.

Exercise 2.2 Let $\mathcal{R}$ be a preorder relation. Show that the relation $\mathcal{R}^\dagger$ defined by $x \mathrel{\mathcal{R}^\dagger} y$ if and only if $x = y$ or $(x \mathrel{\mathcal{R}} y$ and $y \mathrel{\overline{\mathcal{R}}} x)$, where $\overline{\mathcal{R}}$ denotes the complementary of relation $\mathcal{R}$ (see Section 1.4.3), is an ordering. ♢

2.2 Ordered sets

Definition 2.11 *An ordered set $(E, \leq)$ is a set E together with an ordering $\leq$.*

The same set E can be equipped with different orderings. We then have different ordered sets.

Example 2.12 The set of integers $\mathbb{N}$ can be equipped with the usual ordering or with the divisibility ordering of Example 2.3.

2.2.1 Monotonic mappings

Definition 2.13 *Let $(E_1, \leq_1)$ and $(E_2, \leq_2)$ be two ordered sets. A mapping f from E_1 to E_2 is said to be monotonic, or monotone, if*

$$\forall x, y \in E_1, \quad x \leq_1 y \quad \Longrightarrow \quad f(x) \leq_2 f(y).$$

f is also said to be a homomorphism from the ordered set $(E_1, \leq_1)$ to the ordered set $(E_2, \leq_2)$.

$(E_1, \leq_1)$ and $(E_2, \leq_2)$ are said to be isomorphic if there is a bijection b between E_1 and E_2 with the property that both b and b^{-1} are monotone.

Example 2.14

1. If two ordered sets $(E_1, \leq_1)$ and $(E_2, \leq_2)$ have the same underlying set, namely, if $E_1 = E_2$, then the inclusion $\leq_1 \subseteq \leq_2$, i.e. $\forall x, y, \quad x \leq_1 y \Longrightarrow x \leq_2 y$, holds if and only if the identity mapping from E_1 to E_2 is monotone.
2. In order for a bijection to be an isomorphism, monotonicity is not sufficient; for instance, the identity mapping from $(\mathbb{N}, \leq_{\text{div}})$ to $(\mathbb{N}, \leq)$ is a monotone bijection but it is not an isomorphism.

2.2.2 Totally ordered sets

An ordered set $(E, \leq)$ is said to be *totally ordered* if $\leq$ is a total ordering, i.e. if $\forall x, y,\ x \neq y \quad \Longrightarrow \quad x \leq y$ or $y \leq x$. Otherwise, i.e. if $\exists x, y,\ x \neq y,\ x \not\leq y$ and $y \not\leq x$, it is said to be a *partially ordered* set or *poset*. Let $(E, \leq)$ be a partially ordered set. A *linear extension* of $(E, \leq)$ is a totally ordered set $(E, \leq_t)$ with the same underlying set such that $\leq \subseteq \leq_t$.

Theorem 2.15 *Let $(E, \leq)$ be an ordered set. It has at least one linear extension, and $\leq$ is equal to the intersection of all its linear extensions.*

This theorem will not be proved in the general case.

Exercise 2.3 Prove the statement of Theorem 2.15 for the case when E is finite. ♢

2.2.3 Products of ordered sets

Let $(E_1, \leq_1)$ and $(E_2, \leq_2)$ be two ordered sets. The *direct product* of these two ordered sets is $(E_1 \times E_2, \leq)$ with the ordering $\leq$ defined by $(x_1, x_2) \leq (y_1, y_2)$ if and only if $x_1 \leq_1 y_1$ and $x_2 \leq_2 y_2$.

REMARK 2.16
1. The ordering on the direct product is also called the *product ordering*.
2. We can define orderings on $E_1 \times E_2$ other than the product ordering; for instance, we can define $(x_1, x_2) \leq' (y_1, y_2)$ if and only if $y_1 \leq_1 x_1$ and $x_2 \leq_2 y_2$.

EXERCISE 2.4
1. Show that the projections π_i from $E_1 \times E_2$ onto E_i are monotonic.
2. Show that if $|E_1| \geq 2$ and $|E_2| \geq 2$, $E_1 \times E_2$ is not totally ordered even when E_1 and E_2 are.
3. Show that the direct product is associative and commutative up to isomorphism (i.e. the mapping b from $E_1 \times E_2$ to $E_2 \times E_1$ associating (x_2, x_1) with (x_1, x_2) is an isomorphism). ♢

The *lexicographic product* of $(E_1, \leq_1)$ by $(E_2, \leq_2)$ is $(E_1 \times E_2, \leq)$ with $(x_1, x_2) \leq (y_1, y_2)$ if and only if $x_1 < y_1$ or ($x_1 = y_1$ and $x_2 \leq y_2$).

EXERCISE 2.5
1. Show that the lexicographic product of two ordered sets is an ordered set.
2. Show that this product is not commutative, i.e. $(E_1 \times E_2, \leq)$ is not isomorphic to $(E_2 \times E_1, \leq)$.
3. Show that the lexicographic product of total orderings is a total ordering. ♢

2.2.4 Ordered subsets, chains and antichains

Let $(E, \leq)$ be an ordered set. A subordered set of $(E, \leq)$ is an ordered set $(E', \leq')$ such that $E' \subseteq E$ and $\leq' = \leq \cap (E' \times E')$, i.e. $\forall x, y \in E'$, $x \leq' y$ if and only if $x \leq y$.

A *chain* of E is a totally ordered subset of E. A chain is *maximal* if it is not strictly included in another chain.

An *antichain* E' of E is a subset of E such that

$$\leq \cap (E' \times E') \;=\; Id_{E'}\,.$$

In other words, any two elements of an antichain are incomparable, because if they are in the ordering then they must be equal. An antichain is *maximal* if it is not strictly included in any other antichain.

EXERCISE 2.6
1. If $(E, \leq)$ is a totally ordered set then its only antichains are singletons.
2. Show that the intersection of a chain and an antichain has at most one element. ♢

A *left segment* is a subset E' of E such that

$$y \in E' \text{ and } x \leq y \quad \Longrightarrow \quad x \in E'.$$

An *interval* $[x, y]$, with $x \neq y$ and $x \leq y$, is the subset

$$\{z \,/\, x \leq z \text{ and } z \leq y\}\,.$$

An ordered set is *locally finite* if all its intervals are finite.

EXAMPLE 2.17 For the usual ordering on numbers, $\mathbb{N}$ is locally finite and $\mathbb{Q}$ is not.

EXERCISE 2.7 Show that the interval $[x, y]$ is empty if and only if $x \not\leq y$. ♢

We say that x is *covered by* y if interval $[x, y]$ contains only x and y. This relation will be denoted by $x \prec y$.

EXERCISE 2.8 Show that if interval $[x, y]$ is finite then there exists an element of this interval covering x. ♢

Proposition 2.18 *If $(E, \leq)$ is locally finite then $\leq \,=\, \prec^*$.*

EXERCISE 2.9 Prove Proposition 2.18. ♢

2.3 Upper and lower bounds

Definition 2.19 *Let E' be a subset of an ordered set $(E, \leq)$. An element x of E is an upper bound of E' (resp. lower bound) if $\forall y \in E'$, $y \leq x$ (resp. $x \leq y$).*

We denote by $\text{Maj}(E')$ the set of upper bounds of E' and by $\text{Min}(E')$ the set of lower bounds of E'. It is easy to see that $\text{Maj}(\emptyset) = \text{Min}(\emptyset) = E$.

Proposition 2.20 *$Maj(E') \cap E'$ and $Min(E') \cap E'$ each have at most one element.*

Proof. Assume that $\text{Maj}(E') \cap E'$ contains two distinct elements x and y. We thus have $x \leq y$ and $y \leq x$, a contradiction.

The proof is similar for Min. □

If $\text{Maj}(E') \cap E'$ is non-empty then the unique element of this set is called the *greatest element* or *maximum* of E'. Similarly, if $\text{Min}(E') \cap E'$ is non-empty then its unique element is called the *least element* or *minimum* of E'.

Proposition 2.21 *Let E' be a subset of E and let $z \in E$. The following three conditions are equivalent:*

(i) *z is the greatest element of E'.*
(ii) *$z \in E'$ and $\forall x \in E'$, $x \leq z$.*
(iii) *$z \in E'$ and z is the least element of Maj(E').*

The least element of E' has a similar characterization.

Proof.
(i) $\Longrightarrow$ (ii): If z is the greatest element of E', then $z \in E'$ and $z \in \mathrm{Maj}(E')$, and thus (ii) is true.
(ii) $\Longrightarrow$ (iii): $\forall x \in E'$, $\forall y \in \mathrm{Maj}(E')$, $x \leq y$, and thus $E' \subseteq \mathrm{Min}(\mathrm{Maj}(E'))$. Hence $z \in E' \cap \mathrm{Maj}(E') \subseteq \mathrm{Min}(\mathrm{Maj}(E')) \cap \mathrm{Maj}(E')$ and z is the least element of $\mathrm{Maj}(E')$.
(iii) $\Longrightarrow$ (i): The least element of $\mathrm{Maj}(E')$ is in $\mathrm{Maj}(E')$, and thus $z \in E' \cap \mathrm{Maj}(E')$. □

Z Let E' be a subset of E. An element x of E' is said to be *maximal in E'* if $\forall y \in E',\ y \geq x \implies y = x$ or, equivalently, $y \neq x \implies y \not\geq x$. If E' has a greatest element, this greatest element is its unique maximal element, but the converse is false (see Exercise 2.10).

We define the *minimal* elements of a subset E' similarly.

Example 2.22 $\mathbb{N}$ has a minimal element which is its least element (it is 0), but it has no maximal element.

Exercise 2.10
1. Show that if a subset E' of E has a unique maximal element, this element is not necessarily the greatest element of E'.
2. What can you say if E is totally ordered? ♢

Definition 2.23 *An element x is the least upper bound of a subset E' of an ordered set E if*

$$\big(\forall y \in E',\ y \leq x\big) \quad \textit{and} \quad \big(\forall z \in E,\ ((\forall y \in E',\ y \leq z) \implies x \leq z)\big).$$

Similarly, an element x is the greatest lower bound of a subset E' of an ordered set E if

$$\big(\forall y \in E',\ x \leq y\big) \quad \textit{and} \quad \big(\forall z \in E,\ ((\forall y \in E',\ z \leq y) \implies z \leq x)\big).$$

The terminology ‘the’ least upper bound (resp. greatest lower bound) is justified because there is at most one least upper bound (resp. greatest lower bound).

Indeed, the definition of the least upper bound (resp. greatest lower bound) of a subset E' of E is identical to the definition of the least element of $\mathrm{Maj}(E')$ (resp. the greatest element of $\mathrm{Min}(E')$). The least upper bound of subset E' is thus an upper bound of E' that is less than all other upper bounds of E', i.e. the least upper bound of E' is the least among the upper bounds of E'. Similarly, the greatest lower bound of E' is the greatest among the lower bounds of E'.

We denote by $\sup(E')$ and $\inf(E')$ the least upper bound and greatest lower bound, respectively, when they exist.

Proposition 2.24 *Let E' be a subset of E.*

(i) *If z is the greatest element of E', then $z = \sup(E')$.*
(ii) *If $\sup(E') \in E'$, then $\sup(E')$ is the greatest element of E'.*

We have a similar result for the least element and the greatest lower bound of E'.

Proof. This result is a consequence of Proposition 2.21:

(i) If z is the greatest element of E', then z is the least element of $\mathrm{Maj}(E')$. It is thus the least upper bound of E'.
(ii) The least upper bound of E' is the least element of $\mathrm{Maj}(E')$. If it belongs to E' it is thus the greatest element of E'. □

Example 2.25
1. Let $\mathbb{N}$ be ordered by the divisibility relation (see Example 2.3 and Exercise 2.17). For this ordering, the greatest lower bound of a set of two integers always exists and is the greatest common divisor of these two integers. The least upper bound also always exists and is their least common multiple.
2. The least upper bound and the greatest lower bound do not always exist. Consider the set $E = \{a, b, c, d\}$ ordered by : $a \leq c$, $a \leq d$, $b \leq c$, $b \leq d$. See Figure 2.1.

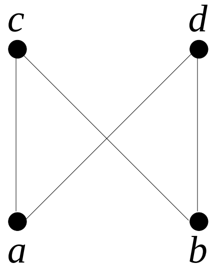

Figure 2.1

Then $\{a, b\}$ has neither a least upper bound nor a greatest lower bound; the same holds for $\{c, d\}$.

Example 2.26 Let $\mathcal{P}(E)$ be the set of subsets of E, ordered by inclusion. Let E_i for $i \in I$ be a family of subsets of E. The least upper bound of this family is $\bigcup_{i\in I} E_i$ and its greatest lower bound is $\bigcap_{i\in I} E_i$.

Proposition 2.27 *Let E_i, for $i \in I$, be a family of subsets of an ordered set and let $E' = \bigcup_{i\in I} E_i$ be its union. If each set E_i has a least upper bound (resp. greatest lower bound) e_i, and if the set $\{e_i \,/\, i \in I\}$ has a least upper bound (resp. greatest lower bound) e, then e is the least upper bound (resp. greatest lower bound) of E'.*

Proof. We show this result only in the case of the least upper bound; the other case is completely similar.

First, we show that e is an upper bound of E'. Let x be any element of E'. It thus belongs to some E_i, and so $x \leq e_i \leq e$.

Now we let z be any upper bound of E' and show that $e \leq z$. Because z is an upper bound of E', it also is an upper bound of E_i, for any i in I, and we have: $\forall i \in I$, $e_i \leq z$. Therefore, because e is the least upper bound of $\{e_i \,/\, i \in I\}$, we have that $e \leq z$. □

2.4 Well-ordered sets and induction

Well-founded sets form the general framework in which we can use proofs by induction. All induction principles stated in Chapter 3 are thus justified by the present section.

Definition 2.28 *An ordered set $(E, \leq)$ is said to be well founded if there is no infinite strictly decreasing sequence of elements of E; $\leq$ is then said to have the well-founded ordering property or to be a well founded ordering. A total ordering $\leq$ having the well-founded ordering property is called a well ordering.*

We now prove an important characterization of well-founded ordered sets.

Proposition 2.29 *An ordered set $(E, \leq)$ is well founded if and only if any non-empty subset of E has at least one minimal element.*

Proof. It is equivalent to show the contrapositive of this result, namely, that $(E, \leq)$ has an infinite decreasing sequence if and only if there exists a non-empty subset having no minimal element. Assume that there exists a strictly decreasing infinite sequence $(x_n)_{n\in\mathbb{N}}$ in E. The set $X = \{x_n \,/\, n \in \mathbb{N}\}$ is a non-empty subset having no minimal element.

Conversely, assume that there exists a non-empty subset having no minimal element. Because X has no minimal element, any element x of X is strictly larger than at least one other element y of X. Thus there exists a function f from X to X verifying $\forall x \in X$, $f(x) < x$. (It suffices to choose one among the elements $y < x$ and to let $f(x) = y$.) Let $x_0 \in X$ (where X is non-empty by hypothesis). For any integer n, we define $x_n = f^n(x_0)$. The sequence $(x_n)_{n\in\mathbb{N}}$ is strictly decreasing because $\forall n \in \mathbb{N}$, $x_n = f(x_{n-1}) < x_{n-1}$. □

Example 2.30

1. The usual ordering is a well ordering on $\mathbb{N}$ but not on $\mathbb{Z}$.
2. $\mathbb{N}^2$ equipped with the product order $\leq$ (see Section 2.2.3) is well founded. Indeed, any element of $\mathbb{N}^2$ has a finite number of lower bounds. Consequently, there can exist no strictly decreasing infinite sequence. More generally, it is easy to see that the product of two well-founded sets is also well founded.
3. The lexicographic ordering $\preceq$ on $\mathbb{N}^2$ is defined by $(n, m) \prec (n', m')$ if and only if $(n < n')$ or $(n = n'$ and $m < m')$. We note that if $n > 0$ then (n, m) has infinitely many lower bounds. For instance, $\forall p \in \mathbb{N}$, $(n-1, p) \prec (n, m)$. Nevertheless, the lexicographic ordering is a well ordering on $\mathbb{N}^2$. Indeed, let X be a non-empty subset of $\mathbb{N}^2$, and let $n = \min\{p \in \mathbb{N} \,/\, \exists q \in \mathbb{N}, (p, q) \in X\}$ and $m = \min\{q \in \mathbb{N} \,/\, (n, q) \in X\}$. We easily verify that (n, m) is the least element of X.

Exercise 2.11 Let $<_1$ be a well ordering on E_1 and let $<_2$ be a well ordering on E_2; we define the *lexicographic product* $\preceq'$ of $<_1$ and $<_2$ on $E_1 \times E_2$ by $(n, m) \prec' (n', m')$ if and only if $(n <_1 n')$ or $(n = n'$ and $m <_2 m')$. Verify that $\preceq'$ is a well ordering on $E_1 \times E_2$. ♢

The induction principle for well-founded sets is stated in the following theorem.

Theorem 2.31 *Let $(E, \leq)$ be a well-founded set and let P be an assertion depending on an element x of E. (P is called a predicate, see Chapter 5.) If the following property is verified:*

$$\text{(I)} \qquad \forall x \in E, \qquad \Big((\forall y < x,\ P(y)) \qquad \Longrightarrow \qquad P(x) \Big),$$

then $\forall x \in E$, $P(x)$.

Proof. Let $X = \{x \in E \,/\, P(x) \text{ is false}\}$. If X is non-empty, X has a minimal element x_0. $\forall y < x_0$, $y \notin X$ and thus $P(y)$ is true. Using (I) we deduce that $P(x_0)$ is true, which contradicts $x_0 \in X$. Thus $X = \emptyset$, which means that $\forall x \in E$, $P(x)$ is true. □

Unfortunately, sets equipped with their natural orderings are not always well founded. We have already seen that $\mathbb{Z}$ with the usual ordering is not well founded. It is of course possible to define well-founded orderings and even well orderings on $\mathbb{Z}$, but these orderings are not very natural. For instance, a well ordering $\preceq$ is defined on $\mathbb{Z}$ by using the usual ordering $\leq$ as follows:

- $\forall n > 0, \forall m > 0,\ n \prec m \iff n < m$ ($\preceq$ coincides with $\leq$ on $\mathbb{N}$).
- $\forall n < 0, \forall m \geq 0,\ n \prec m$ (negative integers are less than positive ones).
- $\forall n < 0, \forall m < 0,\ n \prec m \iff m < n$ (the inverse ordering on negative integers).

Below we give yet another example where the usual ordering is not a well-founded ordering.

Example 2.32 Let A be an alphabet with at least two letters a and b. The free monoid A^*, together with the lexicographic ordering (see Example 2.4), is not well founded. Indeed, $(a^n b)_{n \in \mathbb{N}}$ is a strictly decreasing infinite sequence. Thus, proofs by induction on A^* equipped with the lexicographic ordering will not be valid.

On the other hand, A^* equipped with the *prefix* ordering (Example 2.4) is well founded. Finally, a well ordering on A^* is defined by: $x \prec y$ if and only if

$$(|x| < |y|) \quad \text{or} \quad (|x| = |y| \text{ and } x \prec y \text{ in the lexicographic ordering}).$$

Hence proofs by induction on A^* using either the prefix ordering or the ordering $\prec$ will be valid.

2.5 Complete sets and lattices

2.5.1 Complete sets and continuous functions

Definition 2.33 *An ordered set $(E, \leq)$ is said to be a lattice (resp. complete lattice) if any finite subset (resp. any subset) of E has a least upper bound and a greatest lower bound.*

If E is a lattice, then the greatest lower bound of E is less than any element of E; hence a lattice has a least element that is denoted by $\perp$ and pronounced ‘bottom’. Similarly, a lattice has a greatest element that is denoted by $\top$ and pronounced ‘top’.

Example 2.34 $\mathcal{P}(E)$ ordered by inclusion is a complete lattice.

Exercise 2.12

1. Show that an ordered set $(E, \leq)$ is a lattice if and only if any two-element subset of E has a least upper bound and a greatest lower bound.
2. Show that an ordered set $(E, \leq)$ is a complete lattice if and only if any subset of E has a least upper bound. $\diamondsuit$

Z If an ordered set is a lattice, its least element $\perp$ is also the least upper bound of the empty set. Because the set $\mathrm{Maj}(\emptyset)$ of upper bounds of the empty set is the whole of E, $\perp$ is the least element of E.

Similarly, the greatest element $\top$ is also the greatest lower bound of the empty set.

Definition 2.35 *A mapping f from an ordered set $(E_1, \leq_1)$ to an ordered set $(E_2, \leq_2)$ is said to be continuous (or, more precisely, sup-continuous) if it preserves the least upper bounds of non-empty subsets. In other words, if the subset $E' \neq \emptyset$ has a least upper bound $e = \sup(E')$, then $f(E') = \{f(x) \,/\, x \in E'\}$ also has a least upper bound equal to $f(e)$.*

Remark 2.36 Since the least upper bound of the empty set is $\perp$, the condition 'f preserves the least upper bound of the empty set' is simply $f(\perp_1) = \perp_2$. This is a very exacting requirement that we will not demand for a continuous function.

Since in a complete lattice least upper bounds always exist, the continuity of a mapping between two complete lattices is then simply expressed by:

$$f(\sup(E)) = \sup(f(E)) .$$

Exercise 2.13 Show that any continuous function is monotonic. ♢

Let $C(E)$ be the set of left segments of E ordered by inclusion. Let i be the mapping from E to $C(E)$ defined by $i(x) = \{y \in E \,/\, y \leq x\}$, and let $i(E)$ be the image of E by i.

Proposition 2.37 *$C(E)$ is a complete set. The mapping i is monotonic and is an isomorphism between E and $i(E)$.*

Proof. In order for $C(E)$ to be complete for inclusion, it suffices that any union of left segments is a left segment, and this clearly holds.

If $x \leq y$, it is clear that $i(x) \subseteq i(y)$ and thus i is monotonic.

Conversely, if $i(x) \subseteq i(y)$, then because $x \in i(x)$ we have that $x \in i(y)$ and thus $x \leq y$. Hence $i(x) = i(y)$ implies $x \leq y$ and $y \leq x$, and thus $x = y$. □

However, i is not always continuous, as shown by the next example.

Example 2.38 Let $E = \mathbb{N}$, together with the usual ordering. For $n \in \mathbb{N}$, $i(n) = \{0, 1, \ldots, n\}$, and the only left segment that is not of this form is the whole of $\mathbb{N}$. We can thus identify $C(\mathbb{N})$ with the complete ordered set $\overline{\mathbb{N}} = \mathbb{N} \cup \{\omega\}$, where $\forall n \in \mathbb{N}$, $n < \omega$.

We may again consider the set $C(\overline{\mathbb{N}})$ of left segments of $\overline{\mathbb{N}}$ which is equal to $\{i(n) \,/\, n \in \mathbb{N}\} \cup \{\mathbb{N}, \overline{\mathbb{N}}\}$. The mapping i' from $\overline{\mathbb{N}}$ to $C(\overline{\mathbb{N}})$ is defined by $\forall n \in \mathbb{N}$, $i'(n) = \{0, 1, \ldots, n\}$ and $i'(\omega) = \overline{\mathbb{N}}$. This mapping is not continuous. Indeed, in $\overline{\mathbb{N}}$ the least upper bound of $\mathbb{N}$ is ω, whilst in $C(\overline{\mathbb{N}})$ the least upper bound of the set $\{i'(n) \,/\, n \in \mathbb{N}\}$ is $\mathbb{N}$.

2.5.2 Fixed points of monotone functions

Let f be a mapping from a set E to itself. A *fixed point* of f is an element x of E such that $f(x) = x$.

If E is an ordered set, the set of fixed points of f is a subordered set of E, possibly empty. If this subset has a least element, this least element is called the *least fixed point* of f, and if it has a greatest element, this greatest element is called the *greatest fixed point* of f.

Theorem 2.39 *If f is a monotone mapping from a complete ordered set to itself, then f has a greatest fixed point.*

Proof. We verify that f has a greatest fixed point. Let

$$X = \{x \in E \,/\, x \leq f(x)\}$$

and let $z = \sup(X)$. By the definition of z, we have $\forall x \in X$, $x \leq z$ and hence, since f is monotonic, $f(x) \leq f(z)$. As $x \leq f(x)$, $f(z)$ is an upper bound of X, and hence $z \leq f(z)$. We deduce that $f(z) \leq f(f(z))$, and hence $f(z) \in X$ and thus $f(z) \leq z$. It follows that z is a fixed point of f. If z' is another fixed point, then $z' \in X$ and thus $z' \leq z$. □

Theorem 2.40 *If f is a continuous mapping from a complete ordered set to itself, then f has a least fixed point. This least fixed point is equal to*

$$\sup(\{f^n(\bot) \,/\, n \in \mathbb{N}\}).$$

Proof. Let $x = \sup(\{f^n(\bot) \,/\, n \in \mathbb{N}\})$. Because f is continuous,

$$f(x) = \sup(\{f^{n+1}(\bot) \,/\, n \in \mathbb{N}\}),$$

and because $\bot = f^0(\bot)$ is the least element of E,

$$\sup(\{f^{n+1}(\bot) \,/\, n \in \mathbb{N}\}) = \sup(\{f^n(\bot) \,/\, n \in \mathbb{N}\}) = x,$$

which is thus a fixed point of f. If y is another fixed point of f, we first show by induction that $\forall n \in \mathbb{N}$, $f^n(\bot) \leq y$; because $\bot$ is the least element of E, $\bot = f^0(\bot) \leq y$; if $f^n(\bot) \leq y$ then $f^{n+1}(\bot) \leq f(y) = y$. Hence, $x = \sup(\{f^n(\bot) \,/\, n \in \mathbb{N}\}) \leq y$. □

Theorem 2.41 *If E is a finite ordered set having a least element $\bot$, then for any monotone function f from E to itself there exists $k \leq card(E)$ such that the least fixed point of f is $f^k(\bot)$.*

Proof. Consider the sequence

$$\bot\,,\, f(\bot)\,,\, f^2(\bot)\,,\,\dots\,,\, f^n(\bot)\,,\,\dots\,,$$

which is increasing because f is monotone. If the sequence has two consecutive equal elements then it is stationary:

$$f^i(\bot) = f^{i+1}(\bot) \implies f^{i+1}(\bot) = f^{i+2}(\bot)$$

and thus, by induction, $\forall j \geq i$, $f^i(\bot) = f^j(\bot)$. In the $|E|+1$ first elements of this sequence, there must be two consecutive elements that are equal. We thus have $f^k(\bot) = f^{k+1}(\bot)$ for $k \leq |E|$. The fact that $f^k(\bot)$ is less than any other fixed point of f is proved as in the preceding theorem. □

Exercise 2.14

1. What is the value of $f(\bot)$ if f preserves *all* least upper bounds?
2. If $f(\bot) = \bot$, what is the least fixed point of f? ♢

Exercise 2.15 Consider $\mathcal{P}(E \times E)$ ordered by inclusion. Let $\mathcal{R}$ be a binary relation on E and let f be the mapping of $\mathcal{P}(E \times E)$ to itself defined by $f(X) = Id_E \cup \mathcal{R}.X$.

Show that this mapping is continuous and that its least fixed point is $\mathcal{R}^*$. ♢

2.5.3 Lattices

Definition 2.42 *An ordered set is a lattice (see Definition 2.33 and Exercise 2.12) if any pair of elements has a least upper bound and a greatest lower bound. We will sometimes denote by $x \sqcup y$, instead of $\sup(\{x, y\})$, the least upper bound of x and y, and by $x \sqcap y$ their greatest lower bound.*

Example 2.43 $\mathbb{N}$ equipped with the divisibility ordering is a lattice. The binary operations $\sqcup$ and $\sqcap$ are, respectively, the lcm (least common multiple) and the gcd (greatest common divisor), $\bot$ is 1, and $\top$ is 0. Indeed, 1 divides any number n because $1n = n$, and any number n divides 0 because $n0 = 0$.

Example 2.44 $\mathcal{P}(E)$ together with inclusion is a lattice. The binary operations $\sqcup$ and $\sqcap$ are, respectively, $\cup$ and $\cap$.

If E is a lattice, we may thus consider that E is a set equipped with two binary operations $\sqcup$ and $\sqcap$.

Proposition 2.45 *The operations $\sqcup$ and $\sqcap$ have the following properties:*

- *idempotence: $x \sqcup x = x$ and $x \sqcap x = x$.*
- *commutativity: $x \sqcup y = y \sqcup x$ and $x \sqcap y = y \sqcap x$.*
- *associativity: $(x \sqcup y) \sqcup z = x \sqcup (y \sqcup z)$ and $(x \sqcap y) \sqcap z = x \sqcap (y \sqcap z)$.*
- *absorption: $x \sqcap (x \sqcup y) = x = (y \sqcap x) \sqcup x$.*

Conversely, assume that on a set E there exist two binary operations $\sqcup$ and $\sqcap$ that have the four properties mentioned in the above proposition. Then we can order E in such a way that $x \sqcup y$ and $x \sqcap y$ are, respectively, the least upper bound and the greatest lower bound of x and y. It suffices to let $x \leq y$ if and only if $x \sqcup y = y$, which, because of the absorption property, is equivalent to $x \sqcap y = x$:

$$x \sqcup y = y \Longrightarrow x \sqcap (x \sqcup y) = x \sqcap y \Longrightarrow x = x \sqcap y \ .$$

Since $\sqcup$ is idempotent, $\leq$ is reflexive: from $x \sqcup x = x$ we deduce that $x \leq x$. From the commutativity of $\sqcup$, we easily deduce that $\leq$ is antisymmetric; $x \leq y$ implies $x \sqcup y = y$; $y \leq x$ implies $y \sqcup x = x$; as $x \sqcup y = y \sqcup x$ we have $x = y$. Finally, the transitivity of $\leq$ is an immediate consequence of the associativity of $\sqcup$: $x \leq y \Longrightarrow x \sqcup y = y$; $y \leq z \Longrightarrow y \sqcup z = z$; hence $z = (x \sqcup y) \sqcup z = x \sqcup (y \sqcup z) = x \sqcup z$ and thus $x \leq z$. Moreover, the least upper bound of x and y is indeed $x \sqcup y$: as $x \sqcap (x \sqcup y) = x$, we have $x \leq (x \sqcup y)$, and for the same reasons, $y \leq (x \sqcup y)$; if $x \leq z$ and $y \leq z$, we have $z = x \sqcup z = y \sqcup z$ and thus $z = z \sqcup z = x \sqcup z \sqcup y$, hence $x \sqcup y \leq z$. The fact that the greatest lower bound of x and y is $x \sqcap y$ is proved similarly.

From the associativity and the commutativity of $\sqcup$ and $\sqcap$, it immediately follows that in a lattice, any *finite non-empty* subset has a least upper bound and a greatest lower bound. This can be proved by induction on the number of elements of the finite subset by writing $\{e_1, e_2, \ldots, e_n, e_{n+1}\}$ as the union of two sets $\{e_1, e_2, \ldots, e_n\}$ and $\{e_{n+1}\}$ and by applying Proposition 2.27.

EXERCISE 2.16 Show that both operations $\sqcap$ and $\sqcup$ are monotone, i.e. if $x \leq x'$ and $y \leq y'$ then $x \sqcap y \leq x' \sqcap y'$ and $x \sqcup y \leq x' \sqcup y'$. ♢

Definition 2.46 *A lattice is said to be distributive if $\sqcap$ and $\sqcup$ distribute over each other, i.e. if*

(i) $\forall x, y, z, \quad x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$ *and*
(ii) $\forall x, y, z, \quad x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$.

These two conditions are indeed equivalent. If (i) is true, then (ii) is true. To show this, let us compute

$$(x \sqcap y) \sqcup (x \sqcap z).$$

By (i), this can be written

$$((x \sqcap y) \sqcup x) \sqcap ((x \sqcap y) \sqcup z).$$

By using the absorption property, we obtain

$$x \sqcap ((x \sqcap y) \sqcup z)$$

and, by again applying (i),

$$x \sqcap ((x \sqcup z) \sqcap (y \sqcup z)).$$

By the associativity of $\sqcap$, this is equal to

$$(x \sqcap (x \sqcup z)) \sqcap (y \sqcup z)$$

and, by again using the absorption property, this is equal to

$$x \sqcap (y \sqcup z).$$

The converse implication is proved similarly.

EXAMPLE 2.47 $\mathcal{P}(E)$ is a distributive lattice.

EXAMPLE 2.48 Assume E contains three elements a, b and c pairwise incomparable, a least element $\perp$ and a greatest element $\top$, see Figure 2.2.

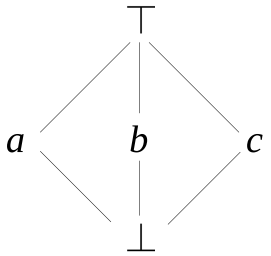

Figure 2.2

It is a lattice because

$$\forall x, y \in \{a, b, c\}\,,\; x \neq y\,,\; x \sqcap y = \perp \text{ and } x \sqcup y = \top.$$

It is not distributive, because

$$a \sqcap (b \sqcup c) = a \sqcap \top = a\ ,$$

while

$$(a \sqcup b) \sqcap (a \sqcup c) = \top \sqcap \top = \top.$$

Definition 2.49 *A lattice E is said to be complemented if*

(i) *it has a least element $\bot$ and a greatest element $\top$, with $\bot \neq \top$ and*
(ii) *there exists a mapping ν from E to E such that*

- $\forall x \in E, \quad x \sqcap \nu(x) = \bot$ *and*
- $\forall x \in E, \quad x \sqcup \nu(x) = \top.$

EXAMPLE 2.50
1. The lattice $\mathcal{P}(E)$ is complemented. Its least element is the empty set, its greatest element is E and the mapping ν is the usual complement operation.
2. The lattice of Example 2.48 is complemented. Let $\nu(\bot) = \top$, $\nu(\top) = \bot$, $\nu(a) = b$, $\nu(b) = c$ and $\nu(c) = a$.

EXERCISE 2.17 The set $\mathbb{N}$ equipped with the divisibility ordering is a lattice.
1. Is it distributive?
2. Is it complemented? ♢

EXERCISE 2.18
1. Show that the set of equivalence relations on a set E is a lattice for inclusion.
2. Is it distributive?
3. Is it complemented? ♢

EXERCISE 2.19 Show that, in a complemented lattice,

$$\nu(\top) = \bot \text{ and } \nu(\bot) = \top.$$ ♢

EXERCISE 2.20 Show that, in a complemented lattice, $\forall x$, $\nu(x) \neq x$. ♢

Proposition 2.51 *If a complemented lattice is distributive, there exists exactly one operation of complement ν. This operation, moreover, verifies*

(i) *involution:* $\forall x, \quad \nu(\nu(x)) = x$,
(ii) *De Morgan's laws:* $\forall x, y, \ \nu(x \sqcup y) = \nu(x) \sqcap \nu(y)$ *and* $\nu(x \sqcap y) = \nu(x) \sqcup \nu(y)$ *and*
(iii) *antimonotonicity:* $x \leq y \quad \Longleftrightarrow \quad \nu(y) \leq \nu(x)$.

Proof.
(i) We first show that in a distributive lattice with a least element and a greatest element, we have the property

$$\forall x, y, z, \quad x \sqcap y = \bot \text{ and } x \sqcup z = \top \quad \Longrightarrow \quad y \leq z.$$

Indeed, $z = z \sqcup \bot = z \sqcup (x \sqcap y) = (z \sqcup x) \sqcap (z \sqcup y) = \top \sqcap (z \sqcup y) = z \sqcup y$, and thus $y \leq z$.

Assume now that there exist two mappings ν and μ verifying

$$\begin{aligned}
\forall x \in E, &\quad x \sqcap \nu(x) = \bot\,,\\
\forall x \in E, &\quad x \sqcup \nu(x) = \top,\\
\forall x \in E, &\quad x \sqcap \mu(x) = \bot\,,\\
\forall x \in E, &\quad x \sqcup \mu(x) = \top.
\end{aligned}$$

Because $x \sqcap \nu(x) = \bot$ and $x \sqcup \mu(x) = \top$, we have that $\nu(x) \leq \mu(x)$. Similarly, $x \sqcap \mu(x) = \bot$ and $x \sqcup \nu(x) = \top$, and hence $\mu(x) \leq \nu(x)$ and thus $\mu(x) = \nu(x)$. Because $\nu(x) \sqcap x = \bot$ and $\nu(x) \sqcup \nu(\nu(x)) = \top$, we have that $x \leq \nu(\nu(x))$, and, for similar reasons, $\nu(\nu(x)) \leq x$.

(ii) In order to show the De Morgan's laws, it suffices to show, taking into consideration the uniqueness of the complement, that

1. $(x \sqcup y) \sqcap (\nu(x) \sqcap \nu(y)) = \bot$ and $(x \sqcup y) \sqcup (\nu(x) \sqcap \nu(y)) = \top$ and
2. $(x \sqcap y) \sqcap (\nu(x) \sqcup \nu(y)) = \bot$ and $(x \sqcap y) \sqcup (\nu(x) \sqcup \nu(y)) = \top$.

We show only the first identity; the second one can be proved similarly:

$$(x \sqcup y) \sqcap (\nu(x) \sqcap \nu(y)) = (x \sqcap \nu(x) \sqcap \nu(y)) \sqcup (y \sqcap \nu(x) \sqcap \nu(y)) = \bot \sqcup \bot = \bot\,.$$

$$(x \sqcup y) \sqcup (\nu(x) \sqcap \nu(y)) = (x \sqcup y \sqcup \nu(x)) \sqcap (x \sqcup y \sqcup \nu(y)) = \top \sqcap \top = \top.$$

(iii) To show the last equivalence, notice that

$$\begin{aligned}
x \leq y \quad &\iff \quad x = x \sqcap y \quad \iff \quad \nu(x) = \nu(x \sqcap y) = \nu(x) \sqcup \nu(y)\\
&\iff \quad \nu(y) \leq \nu(x).
\end{aligned}$$

□

Example 2.52 The lattice of Example 2.48 is not distributive, and there indeed exist at least two operations of complement. For instance $\mu(\bot) = \top$, $\mu(\top) = \bot$, $\mu(a) = c$, $\mu(b) = a$, $\mu(c) = b$.