Chapter 20

Appendix

In this appendix we go through some basic definitions and notations. The notation "$\stackrel{\text{def}}{=}$" ought to be read as "is defined to be", and also " : " stands for the phrase "such that". We sometimes add some notes within the margins, where the notation → means "go to" or "see" what follows this arrow. Also, for the texts appearing in the margins, the abbreviations "Chp.", "Cor.", "Def.", "Exm.", "Exr.", "Fig.", "Not.", "Prt", "Pro.", "Sec." and "Thm." stand for "Chapter", "Corollary", "Definition", "Example", "Exercise", "Figure", "Notation", "Part", "Proposition", "Section" and "Theorem", respectively. An important note of this type is "→ Assumptions" which means that there is a general assumption within the corresponding paragraph. A list of these assumptions can be found in the "Index" section of the book in front of the word "*Assumptions". → Assumptions

20.1 Primitive concepts and notations

20.1.1 Numbers and sets

Intuitively, a *set* is a well-defined collection of distinct objects (for more on set theory[1] e.g. see []). Each of these objects is called an *element* or a *member* of the set. Sometimes, the words *collection* and *family* are also used instead of set; but these words are usually used to indicate sets whose elements are also sets or not necessarily distinct. Sets are usually referred to by capital Latin letters where their elements are referred to by lower case ones. The notation $a \in A$ means that a is an element of the set A and $a \notin A$ indicates the opposite meaning. The size of a finite set A is denoted by $|A|$. → cardinality

The sets of natural numbers, integers, rationals and reals are denoted by $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, respectively. For any real number $r \in \mathbb{R}$ we define the positive part of r, denoted by $(r)^+$, as

$$(r)^+ \stackrel{\text{def}}{=} \begin{cases} r & r > 0 \\ 0 & r \leq 0. \end{cases}$$

The real number $(r)^-$ is defined similarly. Also, $\lfloor r \rfloor$ stands for the largest integer that is less than or equal to the real number r. Similarly, $\lceil r \rceil$ stands for the smallest integer that is greater than or equal to r.

Note that throughout this book the set of natural numbers, $\mathbb{N}$, contains the element zero denoted by 0. However, if we need to refer to positive (i.e. nonnegative and nonzero) elements, we add a + sign as a superscript. For instance, $\mathbb{N}^+$ refers to the set of positive natural numbers.

[1] Although we try to be mathematically correct, but we do not intend to explain, in an axiomatic way, all the details of a suitable *set theory* for what we need throughout the book. Section 20.1 mainly follows Zermelo-Fraenkel set theory with axiom of choice added (i.e. ZFC), however, a student will not be needing the details of such set systems. A better choice could be von Neumann-Bernays-Gödel (i.e. NBG) set theory that will be used in Section 20.2, in which, intuitively, a student may always assume that the whole thing is happening in a large enough universal set/class. What makes NBG more suitable for our context is the fact that it is finitely axiomatizable. Anyhow, non of the details of such set systems affect our arguments in this book unless it is explicitly stated otherwise.

DRAFT

Also, for natural numbers $m, n \in \mathbb{N}$ with $m \leq n$ we define $[\![m, n]\!] \overset{\text{def}}{=} \{m, m+1, \ldots, n\}$ and for $n \in \mathbb{N}^+$ we define $[\![n]\!] \overset{\text{def}}{=} [\![1, n]\!]$.

A set without any element is called an *empty set* or a *void set* and is denoted by $\emptyset$. When each member of a set A is also an element of a set B, we say that A is a *subset* of B and we write $A \subseteq B$. Similarly, we write $A \supseteq B$ if A is a superset of B. The expressions $A \subset B$ and $A \supset B$ indicate that A is a subset or a superset which is not equal to B itself, respectively. Clearly, every set is a subset of itself and the empty set is a subset of any set. For a set A, the subsets A and $\emptyset$ are called the *trivial subsets* of A. Also, the family of all subsets of A is called the *power set* of A and is denoted by $\mathcal{P}(A)$. If A and B are two sets, $B \subseteq A$ and $B \neq A$, then we say that B is a *proper* subset of A. Two sets A and B are said to be *equal* if $A \subseteq B$ and $B \subseteq A$. This equality is denoted by the notation $A = B$. Note that each set is determined completely by its members; thus, A and B are equal only when they contain the same elements.

If p and q are two mathematical propositions, p *and* q is a proposition which is true if and only if both p and q are[2] true. Also, p *or* q is a proposition which is true if and only if at least one of the propositions p and q is true. The proposition $p \Rightarrow q$ is false only when p is true and q is false, and one reads "p implies q". The proposition $p \Leftrightarrow q$ is equivalent to $(p \Rightarrow q)$ *and* $(q \Rightarrow p)$ and therefore is true if and only if both propositions $p \Rightarrow q$ and $q \Rightarrow p$ are true, while one reads "p if and only if q" or "p and q are equivalent". If A is a set and $p(x)$ is a proposition or a property about $x \in A$, then the notation $\exists\ x \in A,\ p(x)$ means that there is at least one element a in A for which $p(a)$ is true. Similarly, $\exists!\ x \in A,\ p(x)$ stands for "there exists a unique" quantifier. Finally, $\forall\ x \in A,\ p(x)$ means that for each member a in A, $p(a)$ is a true proposition.

Sets are usually written in the form $\{x \in U \ : \ p(x)\}$ in which $p(x)$ is a proposition or property of a variable x in U where the set U is the universe or the universal set. Hence, $A = \{x \in U \ : \ p(x)\}$ means that A is the subset of all elements of U for which $p(x)$ is true; e.g. if $\mathbb{N} \overset{\text{def}}{=} \{0, 1, 2, 3, \ldots\}$ is the set of all natural numbers, then the set of all even natural numbers can be represented as $\{x \in \mathbb{N} \ : \ \exists\ y \in \mathbb{N},\ \ x = 2y\}$.

20.1.2 Relations and functions

Roughly speaking, if we order the members of a two-element set such that one of them is regarded as the first and the other as the second member of the set, then we have an *ordered pair* of the members of the set. In this case, if $\{a, b\}$ is a two-element set and we choose a and b as the first and second members, respectively, then the ordered pair (a, b) is obtained and vice versa, if b and a are chosen as the first and the second elements, respectively, then we have the ordered pair (b, a). Any definition for an ordered pair (a, b) is acceptable, if, firstly, the definition indicates exactly that a is the first and b is the second member of the set $\{a, b\}$, and secondly, two ordered pairs (a, b) and (c, d) are equal if and only if $a = c$ and $b = d$; e.g. (a, b) can be defined as the set $\{\{a\}, \{a, b\}\}$ from which it is clear that a is the first and b is the second member and the condition $[(a, b) = (c, d)] \Leftrightarrow [a = c, b = d]$ is also satisfied. This definition can easily be generalized to any finite number of elements; e.g. the *ordered triple* (a, b, c) is defined as $((a, b), c)$ in which a, b and c are respectively the first, the second and the third members of a set $\{a, b, c\}$. Hence, an *ordered quadruple* (a, b, c, d) may be defined as $((a, b, c), d)$ and so on.

If A and B are two sets, the *Cartesian product* of A and B is denoted by $A \times B$ and is defined as follows

$$A \times B = \{(a, b) \ : \ a \in A, b \in B\},$$

i.e. $A \times B$ is the set of all ordered pairs (a, b) in which $a \in A$ and $b \in B$. This definition can also be extended to any finite number of sets; i.e. if $A_1, A_2, \ldots, A_n$ are a finite number of sets, the Cartesian product $A_1 \times A_2 \times \ldots \times A_n$ is defined as

$$\{(a_1, a_2, \ldots, a_n) \ : \ a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

Clearly, $A_1 \times \ldots \times A_n = \emptyset$ if and only if at least one of the sets A_1, A_2, $\ldots$, and A_n is an empty set. Also, A^n stands for the Cartesian product of n copies of A.

[2] Occasionally, one may use the notations "," or "&" instead of Roman "and" in mathematical expressions.

DRAFT

A *relation* R from a set A to another set B is a subset of $A \times B$. If $A = B$, then we say that R is a relation *in* A. If R is a relation from A to B, we write aRb to show that $(a, b) \in R$ and in this case we say that a is related to b by (or through) R.

Let R be a relation from A to B. The *domain* of R is denoted by $dom(R)$ and is defined as

$$dom(R) \stackrel{\text{def}}{=} \{x \in A \ : \ \exists\, y \in B,\ (x, y) \in R\}.$$

The *range* or *image* of R is denoted by $im(R)$ or $ran(R)$ and is defined as

$$im(R) = ran(R) \stackrel{\text{def}}{=} \{y \in B \ : \ \exists\, x \in A,\ (x, y) \in R\}.$$

If R is a relation in A and $dom(R) = A$, then we say that "R is a relation *on* A" or that "R is a *total relation* in A". A relation R from A to B is said to be *locally finite* if

$$\forall\, x \in A, \quad |\{y \in B \ : \ (x, y) \in R\}| < \infty.$$

Also, the *inverse* of R is denoted by R^{-1} and is defined as → Exr. 20.3.1

$$R^{-1} \stackrel{\text{def}}{=} \{(y, x) \in B \times A \ : \ (x, y) \in R\}.$$

It is obvious that $\left(R^{-1}\right)^{-1} = R$.

Let R be a relation from X to Y and S a relation from Y to Z. The *composition* of R and S is defined to be a relation $S \circ R$ such that

$$S \circ R \stackrel{\text{def}}{=} \{(x, z) \in X \times Z \ : \ \exists\, y \in Y,\ (x, y) \in R \text{ and } (y, z) \in S\}.$$

It is easy to verify that for every three relations R from W to X, S from X to Y and T from Y to Z we always have

$$T \circ (S \circ R) = (T \circ S) \circ R \quad (\textit{the associative law}),$$

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1}.$$

If R is a relation on a set X, then

- R is said to be *reflexive*, if for every $x \in X$ we have xRx.
- R is said to be *symmetric*, if xRy implies yRx for all $\{x, y\} \subseteq X$.
- R is said to be *transitive*, if xRy and yRz imply xRz for all $\{x, y, z\} \subseteq X$.
- R is said to be *antisymmetric*, if xRy and yRx imply $x = y$ for all $\{x, y\} \subseteq X$.

A *partial function* f (or a *function* f for short) from A to B, denoted by $f : A \longrightarrow B$, is a relation from A to B such that for each $a \in A$ there is at most one pair (a, b) in R. We say that $f(a)$ is *defined* if $x \in dom(f)$, and that $f(a)$ is *undefined* if $[a \notin dom(f) \text{ and } a \in A]$. In this situation, to explain the rule, one may write $a \mapsto f(a)$, or one may explicitly define f as

$$f : A \longrightarrow B, \quad f(a) \stackrel{\text{def}}{=} \begin{cases} b & a \in dom(f) \text{ and } (a, b) \in f \\ \text{undefined} & a \notin dom(f) \text{ and } a \in A. \end{cases}$$

If one also verifies that $dom(f) = A$, which means that f is defined for all $a \in A$, then the function f is referred to as a *total function* or a *map* or a *mapping*, where we may use the notation $f : A \bullet\!\!\longrightarrow B$ for this concept to emphasize this situation. By definition, two functions $f : A \longrightarrow B$ and $g : A \longrightarrow B$ are equal, if and only if, they are equal as relations in $A \times B$. Since $\emptyset \times \emptyset = \emptyset$, the empty set can be regarded as a partial function with an empty domain. If $f : A \longrightarrow B$ and $g : X \longrightarrow Y$ are two functions, then f and g are in fact two sets (i.e. as relations) and therefore it is meaningful if one asks about whether one of them is a subset of the other. If $f \subseteq g$, then we say that "f is a *restriction* of g" or that "g is an *extension* of f".

DRAFT

It is obvious that f is a restriction of g, if and only if, firstly, $dom(f) \subseteq dom(g)$, and secondly, for every $x \in dom(f)$ we have $f(x) = g(x)$.

Usually, when $g : X \longrightarrow Y$ is a function and $A \subseteq X$, then the *restriction of g to A* is denoted by $g|_A$; i.e. → Exr. 20.3.6

$$g|_A \stackrel{\text{def}}{=} \{(x, y) \in f \quad : \quad x \in A\}.$$

Let $f : X \longrightarrow Y$ be a function. For each $A \subseteq X$, the set $f(A)$ is called the *image* of A by f and is defined as

$$f(A) \stackrel{\text{def}}{=} \{y \in ran(f) \ : \ \exists x \in A, \quad y = f(x)\},$$

in which case one may write $f(A) = ran(f|_A)$. For each $B \subseteq Y$, the set $f^{-1}(B)$ is called the *inverse image* of B under f and is defined as

$$f^{-1}(B) \stackrel{\text{def}}{=} \{x \in dom(f) \quad : \quad f(x) \in B\}.$$

For a set A, a total function $f : A \bullet\!\!\longrightarrow A$ is said to be the *identity function* on A, if for each $x \in A$ we have $f(x) = x$. In fact, the identity function on A is $\{(x, x) \quad : \quad x \in A\}$ which is denoted by Id_A.

If A and B are two sets, then a total function $f : A \bullet\!\!\longrightarrow B$ is called a *constant function* , if for each $x \in A$, we have $f(x) = b$ for a fixed member $b \in B$; i.e. a constant function is a total function that maps all members to a fixed member of the range. In other words, the above constant function is in fact the Cartesian product $A \times \{b\}$. The symbols $\mathbf{1}_A$ and $\mathbf{0}_A$ stand for the constant functions equal to one and zero on A, respectively.

Given a set $A \subseteq U$, the symbol χ_A stands for a total function called the characteristic function of the set A (with respect to U). Moreover, χ_a denotes the characteristic function of the subset $\{a\} \subseteq U$ when we always assume that the universe U is clear from the context, i.e.

$$\chi_A(x) \stackrel{\text{def}}{=} \begin{cases} 1 & x \in A \\ 0 & otherwise, \end{cases} \qquad \text{and} \qquad \chi_a(x) \stackrel{\text{def}}{=} \begin{cases} 1 & x = a \\ 0 & otherwise. \end{cases}$$

A function $f : X \longrightarrow Y$ is said to be *one to one*, if $x_1 \in dom(f)$, $x_2 \in dom(f)$ and $x_1 \neq x_2$ imply $f(x_1) \neq f(x_2)$ or equivalently, from $f(x_1) = f(x_2)$ it follows that $x_1 = x_2$, in which case we may use the notation $f : A \stackrel{1-1}{\longrightarrow} B$ to emphasize this situation. One of the simplest one to one and total functions is the identity function on a set X. The total function $f : X \bullet\!\!\longrightarrow \mathcal{P}(X)$ with the rule $f(x) = \{x\}$ is also one to one. → Exr. 20.3.2

A function $f : X \longrightarrow Y$ is said to be an *onto*, if $ran(f) = Y$; i.e. for each $y \in Y$ there is at least one $x \in X$ with $f(x) = y$, in which case we may use the notation $f : A \longrightarrow\!\!\bullet\ B$ to emphasize this situation. In this case, we say that f is a function from X *onto* Y.

If a total function $f : X \bullet\!\!\longrightarrow Y$ is both one to one and onto, then we say that f establishes a *one to one correspondence* between X and Y, in which case we may use the notation $f : A \longleftrightarrow B$ to emphasize this situation. In this setup, when $X = Y$, then one says that f is a *permutation* on X.

The set of functions from a set A to a set B is denoted by $\mathscr{F}(A, B)$, while the set of total functions from A to B is denoted by B^A. → Exr. 20.3.5

If $f : X \to Y$ and $g : Y \to Z$ are two (partial) functions, then f and g are also two relations and therefore, one may talk about their composition as two relations; i.e. $g \circ f$ is a function from X to Z and for every $x \in X$ we have,

$$(g \circ f)(x) \stackrel{\text{def}}{=} \begin{cases} g(f(x)) & \text{if f(x) and g(f(x)) are both defined,} \\ \text{undefined} & \text{otherwise.} \end{cases}$$

This partial function is called the *composition* of f and g. The following statements are some corollaries of the previous definitions. → Sec. 20.2

i) If $f : X \longrightarrow Y$ is a function and there is a function $g : Y \longrightarrow X$ with $g \circ f = Id_{dom(f)}$, then f is one to one.

ii) If $f : X \longrightarrow Y$ is a function and there is a function $g : Y \longrightarrow X$ with $g \circ f = Id_X$, then f is one to one and total.

DRAFT

iii) If $f : X \longrightarrow Y$ is a function and there is a function $h : Y \longrightarrow X$ with $f \circ h = Id_{_Y}$, then f is onto.

iv) The composition of functions has the property of association; i.e. if A, B, C, and D are sets, then for every three functions $f : A \longrightarrow B$, $g : B \longrightarrow C$ and $h : C \longrightarrow D$ we have

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

If $f : X \longrightarrow Y$ is a function, then f is also a relation. Now, if f^{-1}, i.e. the set $\{(y, x) \in Y \times X : (x, y) \in f\}$ is also a function, then we say that f is *invertible* and f^{-1} is the *inverse* of f. The following propositions can be derived from former concepts and definitions.

i) A function $f : X \longrightarrow Y$ is invertible, if and only if f is one to one.

ii) Let $f : X \longrightarrow\!\!\!\!\bullet\, Y$ be an invertible and onto function whose inverse is $f^{-1} : Y \longrightarrow X$. Then $f^{-1} \circ f = Id_{_{dom(f)}}$ and $f \circ f^{-1} = Id_{_Y}$.

iii) Let $f : X \longrightarrow Y$ be a function. Also, assume that there are two functions $g : Y \longrightarrow X$ and $h : Y \longrightarrow X$ such that $g \circ f = Id_{_X}$ and $f \circ h = Id_{_Y}$. Then, f is total, invertible and onto. In addition, we have $g = h = f^{-1}$.

iv) When a function is invertible, then its inverse is unique.

Two sets A and B are said to be *equivalent*, if and only if there exists a one to one correspondence between them. In this case, we write $A \sim B$.

Definition 1.20.1 Cardinality of sets We say that two sets A and B have the same *cardinality* if and only if $A \sim B$. ▶

If $k \in \mathbb{N} \stackrel{\text{def}}{=} \{0, 1, 2, 3, \ldots\}$, then we define $\mathbb{N}_{_0} \stackrel{\text{def}}{=} \emptyset$ and for $k \geq 1$, $\mathbb{N}_{_k} \stackrel{\text{def}}{=} \{0, 1, \ldots, k-1\}$. A set A is said to be *finite*, if and only if there is a natural number $k \geq 0$ such that $A \sim \mathbb{N}_{_k}$, in which case we say that the cardinality of A is equal to k and write $|A| = k$. If a set A is not finite, we say that A is *infinite*.

The cardinality of $\mathbb{N}$ is defined to be $\aleph_{_0}$, read "aleph naught". A set A is said to be *countable*, if either A is finite or it is equivalent to the set of natural numbers $\mathbb{N}$. Otherwise, we say that A is *uncountable*. Note that, one of the most important countable sets is the set of *rational* numbers denoted usually by $\mathbb{Q}$ which is defined as $\mathbb{Q} \stackrel{\text{def}}{=} \{m/n \quad : \quad m, n \in \mathbb{Z},\ n \neq 0\}$ in which $\mathbb{Z}$ denotes the set of *integers* defined as $\mathbb{Z} \stackrel{\text{def}}{=} \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.

Here, we list some important properties for further reference. For more on set theory and the theory of cardinals e.g. see [].

Proposition 2.20.1 Some basic properties of Cardinal numbers

i) *The equivalence of sets, $\sim$, is an equivalence relation.*

ii) *If $A \sim B$ then $\mathcal{P}(A) \sim \mathcal{P}(B)$.*

iii) *If $|A| = \aleph_{_0}$ and A is equivalent to a subset of $\mathbb{N}$, then A is equivalent to $\mathbb{N}$ itself.*

iv) *The union of any two countable sets is countable.*

v) *The set $\mathcal{P}(\mathbb{N})$ is not countable.*

20.1.3 Operations on sets

Let I be an arbitrary set and X a family of sets. If f is a one to one correspondence between I and X; i.e. f is a one to one and onto map from I to X, then we say that the collection of sets X is indexed by I and X is called an *indexed family* of sets. In this case, the image by f of an element $i \in I$ is denoted by $A_{_i}$, where we write $X \stackrel{\text{def}}{=} \{A_{_i}\}_{_{i \in I}}$. Here, if $I = [\![n]\!]$, one may also use the notation $\{A_{_i}\}_{_{i=1}}^{n}$.

For any two sets A and B, the *union* of two sets A and B which is denoted by $A \cup B$, is defined as

$$A \cup B \stackrel{\text{def}}{=} \{x \quad : \quad x \in A \ \ or \ \ x \in B\}.$$

DRAFT

Likewise, the union of n ($n \in \mathbb{N}$) sets $A_1, \ldots, A_n$ is denoted by $A_1 \cup \ldots \cup A_n$ or $\bigcup_{i=1}^{n} A_i$ and is defined as

$$\bigcup_{i=1}^{n} A_i \stackrel{\text{def}}{=} \{x \quad : \quad x \in A_1 \text{ or} \ldots \text{ or } x \in A_n\}.$$

In general, if $\{A_i\}_{i \in I}$ is an indexed collection of sets, then the union of these sets which is represented by $\bigcup_{i \in I} A_i$, is defined as follows

$$\bigcup_{i \in I} A_i \stackrel{\text{def}}{=} \{x \quad : \quad \exists\, i \in I,\ x \in A_i\};$$

i.e. $\bigcup_{i \in I} A_i$ is the set of all elements belonging to at least one of the sets A_i. If $I = \mathbb{N}$, one may write $\bigcup_{i=1}^{\infty} A_i \stackrel{\text{def}}{=} \bigcup_{i \in I} A_i$. Also, if X is a family of sets, then we define

$$\bigcup_{B \in X} B \stackrel{\text{def}}{=} \{x \quad : \quad \exists\, B \in X,\ x \in B\}.$$

The *intersection* of A and B is denoted by $A \cap B$ and is defined as

$$A \cap B \stackrel{\text{def}}{=} \{x \quad : \quad x \in A \text{ and } x \in B\}.$$

Similarly, the intersection of n sets $A_1, \ldots, A_n$ is represented by $A_1 \cap \ldots \cap A_n$ or $\bigcap_{i=1}^{n} A_i$ and is defined as

$$\bigcap_{i=1}^{n} A_i \stackrel{\text{def}}{=} \{x \quad : \quad x \in A_1, \ldots, x \in A_n\}.$$

In general, if $\{A_i\}_{i \in I}$ is a family of sets, then their intersection is denoted by $\bigcap_{i \in I} A_i$ and is defined as follows

$$\bigcap_{i \in I} A_i \stackrel{\text{def}}{=} \{x \quad : \quad \forall\, i \in I,\ x \in A_i\};$$

i.e. $\bigcap_{i \in I} A_i$ is the set of those elements that belong to every A_i. Similarly, when $I = \mathbb{N}$, one may write $\bigcap_{i=1}^{\infty} A_i \stackrel{\text{def}}{=} \bigcap_{i \in I} A_i$. In particular, if the indexing set I is the empty set, then it follows from the definitions that

$$\bigcup_{i \in I} A_i = \emptyset.$$

If X is a collection of sets, then we define

$$\bigcap_{B \in X} B \stackrel{\text{def}}{=} \{x \quad : \quad \forall B \in X, \quad x \in B\}.$$

Two sets A and B are said to be *disjoint*, when $A \cap B = \emptyset$. A family of sets $\{A_i\}_{i \in I}$ are said to be *pairwise disjoint*, if for every $i \in I$ and $j \in I$ with $i \neq j$, $A_i \cap A_j = \emptyset$.

Using the definitions, one may easily verify the following facts for every three sets A, B and

DRAFT

C.

$A = A \cap A$ and $A = A \cup A$. (*idempotency*)
$A \cap B = B \cap A$ and $A \cup B = B \cup A$. (*commutative laws*)
$A \cap (B \cap C) = (A \cap B) \cap C$ and $A \cup (B \cup C) = (A \cup B) \cup C$. (*associative laws*)
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. (*distributive laws*)
$A \subseteq B \Leftrightarrow A \cup B = B \Leftrightarrow A \cap B = A$.

In general, if A is a set and $\{A_i\}_{i\in I}$ a collection of sets, then

$$A \cap (\bigcup_{i\in I} A_i) = \bigcup_{i\in I} (A \cap A_i),$$

$$A \cup (\bigcap_{i\in I} A_i) = \bigcap_{i\in I} (A \cup A_i).$$

If A and B are two sets, the *difference* of A and B which we denote by $A - B$ is defined as

$$A - B \stackrel{\text{def}}{=} \{x \in A \quad : \quad x \notin B\}.$$

If $A \subseteq B \subseteq U$, then $B - A$ is said to be the *complement* of A with respect to B. In particular, the complement of a set A with respect to U is denoted by A^c.

We conclude from the above definitions that if A and B are two arbitrary sets, then

$$(A \cap B)^c = A^c \cup B^c \text{ and } (A \cup B)^c = A^c \cap B^c, \quad (De\ Morgan\ laws)$$

$$\emptyset^c = U,\ U^c = \emptyset \text{ and } (A^c)^c = A,$$

and generally, if $\{A_i\}_{i\in I}$ if a family of sets, then

$$(\bigcap_{i\in I} A_i)^c = \bigcup_{i\in I} {A_i}^c \text{ and } (\bigcup_{i\in I} A_i)^c = \bigcap_{i\in I} {A_i}^c. \quad (generalized\ De\ Morgan\ laws)$$

Let f be a function from X to Y. If $\{A_i\}_{i\in I}$ is a family of subsets of X and A and B are arbitrary subsets of X, then

i) $A \subseteq B \Rightarrow f(A) \subseteq f(B)$.

ii) $f(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} f(A_i)$.

iii) $f(\bigcap_{i\in I} A_i) \subseteq \bigcap_{i\in I} f(A_i)$.

iv) $A \cap dom(f) \subseteq f^{-1}(f(A))$.

If $\{B_i\}_{i\in I}$ is a collection of subsets of Y and B and C are subsets of Y, then

i) $B \subseteq C \Rightarrow f^{-1}(B) \subseteq f^{-1}(C)$.

ii) $f^{-1}(\bigcup_{i\in I} B_i) = \bigcup_{i\in I} f^{-1}(B_i)$.

iii) $f^{-1}(\bigcap_{i\in I} B_i) = \bigcap_{i\in I} f^{-1}(B_i)$.

iv) $f^{-1}(B - C) = f^{-1}(B) - f^{-1}(C)$.

v) $f^{-1}(B^c \cap Y) = X \cap (f^{-1}(B))^c$.

DRAFT

vi) $f(f^{-1}(B)) \subseteq B$.

For any two sets A and B the *symmetric difference* of A and B which is denoted by $A\Delta B$, is defined to be

$$A\Delta B \stackrel{\text{def}}{=} (A - B) \cup (B - A).$$

Also, for every two sets A and B we have

i) $A\Delta A = \emptyset$.

ii) $A\Delta B = B\Delta A$. (*commutativity*)

iii) $A\Delta U = A^c$ and $A\Delta\emptyset = A$.

Moreover, for any three sets A, B and C we have

$$A \cap (B\Delta C) = (A \cap B)\Delta(A \cap C). \quad (\textit{distribution of } \cap \textit{ with respect to } \Delta)$$

$$A\Delta(B\Delta C) = (A\Delta B)\Delta C. \quad (\textit{associativity})$$

Concerning Cartesian products, the symbol A^n stands for the Cartesian product of n copies of the set A, and $A^{(n)}$ is defined as,

$$A^{(n)} \stackrel{\text{def}}{=} \bigcup_{1 \leq m \leq n} A^m.$$

A relation $R \subseteq A^{(n)} \times B^{(n)}$ is said to be a *graded relation* if for any $1 \leq k \leq n$,

$$(a, b) \in R \text{ and } a \in A^k \Rightarrow b \in B^k.$$

Also, note that any such graded relation can be identified with a subset $R \subseteq (A \times B)^{(n)}$ that we denote by the same notation R for clarity. Hence, in this setting, given a relation $S \subseteq A \times B$, one may talk about a graded relation $R \subseteq S^{(n)} \subseteq (A \times B)^{(n)}$.

20.1.4 Equivalence relations and partitions

A relation R on a set A is said to be an *equivalence* relation, if R is reflexive, symmetric and transitive. As an example, the *equality relation* on a nonempty set A defined as

$$Id_A \stackrel{\text{def}}{=} \{(x, x) \quad : \quad x \in A\}$$

is itself an equivalence relation contained in every other equivalence relation. Suppose that R is an equivalence relation on a nonempty set A. If $a \in A$, we define

$$[a]_R \stackrel{\text{def}}{=} \{b \in A \quad : \quad aRb\}.$$

The set $[a]_R$ is called the *equivalence class* of a or equivalence class containing a with respect to the relation R. Note that $[a]_R \neq \emptyset$, since R is reflexive. Each one of the members of $[a]_R$ is said to be a *representative* for the equivalence class containing a. The collection of all equivalence classes of members of A is denoted by A/R. Therefore, we define $A/R \stackrel{\text{def}}{=} \{[a]_R \quad : \quad a \in A\}$. → Exr. 20.3.3 → Exr. 20.3.4

An important example is the case of an onto map $\sigma : A \twoheadrightarrow B$ that gives rise to an equivalence relation $\sim_\sigma$ on A according to which → Sec. 7.3

$$a_1 \sim_\sigma a_2 \Leftrightarrow \sigma(a_1) = \sigma(a_2).$$

The set of k-subpartitions of a set A, $\mathcal{D}_k(A)$, is defined to be the set of all k-sets $\{B_1, \ldots, B_k\}$ with $\emptyset \neq B_i \subseteq A$ for all $1 \leq i \leq k$ such that for every pair $1 \leq i < j \leq k$ we have $B_i \cap B_j = \emptyset$. The set of k-partitions of a set A, which is denoted by $\Pi_k(A)$, is the subset of $\mathcal{D}_k(A)$ that contains all partitions $\{B_1, \ldots, B_k\}$ for which $\cup_{i=1}^k B_i = A$. The sets of all subpartitions and partitions of a set A are denoted by $\mathcal{D}(A)$ and $\Pi(A)$, respectively.

The following important theorem and the following corollary connects the concepts partitions to equivalence relations.

DRAFT

Theorem 3.20.1 *If R is an equivalence relation on a nonempty set A, then for every $a_1 \in A$ and $a_2 \in A$ we have*

$$[a_1]_R \cap [a_2]_R \neq \emptyset \Leftrightarrow [a_1]_R = [a_2]_R \Leftrightarrow a_1 R a_2.$$

in other words, every two equivalence classes are either equal or are disjoint and every $a \in A$ belongs to one and only one equivalence class; i.e. to $[a]_R$.

Corollary 4.20.1 *If R is an equivalence relation on a nonempty set A, then A/R is a partition of A.*

Note that the above theorem states in fact that two members a_1 and a_2 are related together by R, if and only if, both of them are located in a same equivalence class and since the above corollary implies that these equivalence classes constitute a partition, therefore, two elements $[a_1]_R$ and $[a_2]_R$ are related together, if and only if, they belong to the same class of the partition. This fact suggests that the converse of the previous corollary is also true; i.e. whenever we have a partition ζ on a set A, an equivalence relation can be made from it in the following way.

Theorem 5.20.1 *Let $\zeta \in \Pi(A)$ be a partition of a nonempty set A. Then, the relation R defined on A as follows, is an equivalence relation on A and the collection of equivalence classes obtained from this equivalence relation, is exactly the partition ζ,*

$$a_1 R\ a_2 \Leftrightarrow \exists\ B \in \zeta,\ a_1 \in B \text{ and } a_2 \in B.$$

The second part of the above theorem states in fact that $A/R = \zeta$. Usually, it is convenient to denote this specific relation R, by the notation A/ζ. With this terminology, within the above context may write

$$A/(A/\zeta) = \zeta.$$

20.1.5 Partial orders and well-ordered sets

Definition 6.20.1 Given a nonempty set X, a *preorder* on a set X is a relation on X which is reflexive and transitive. ▶

Preorders are usually denoted by "$\leq$". Therefore, a preorder such as $\leq$ on X is a relation on X such that for every three members x, y and z in X, we have

$$x \leq x,$$

$$(x \leq y,\ y \leq z) \Rightarrow x \leq z.$$

A *preordered set* is an ordered pair $(A, \leq)$ in which A is a nonempty set and $\leq$ is a preorder on A. If x and y are two elements of a preordered set, then $y \geq x$ means that $x \leq y$. Also, $x < y$ is equivalent to $x \leq y$ *and* $x \neq y$. The symbol $y > x$ is defined similarly. If $x < y$, we say that x is *strictly smaller* than y or y is *strictly greater* than x.

If $\leq$ is a preorder on X and $Y \subseteq X$, then the set of ordered pairs (a, b) such that $a \in Y$ and $b \in Y$ and $(a, b) \in \leq$ (i.e. $a \leq b$), obviously constitutes a preorder on Y. This preorder is said to be the *induced preorder* from X to Y. Since we usually indicate preorders by $\leq$, when we speak about preordered sets $(A, \leq)$ and $(B, \leq)$, we assume that the difference between the preorders are clear from the context.

Definition 7.20.1 A *partially ordered relation* or *partial order* on a set X is a preorder on X which is also antisymmetric. ▶

A *partially ordered set* or briefly a *poset* is an ordered pair $(A, \leq)$ in which A is a nonempty set and $\leq$ is a partial order on A. If $\leq$ is a partial order on X and $Y \subseteq X$, then one may also talk about the *induced partial order* from X to Y.

Example 8.20.1 Let $\mathcal{F}$ be a nonempty family of sets. The "inclusion" relation in $\mathcal{F}$ is defined as,

$$\subset_{\mathcal{F}} \stackrel{\text{def}}{=} \{(A, B) \in \mathcal{F} \times \mathcal{F}\ :\ A \subset B\}.$$

DRAFT

Then $(\mathcal{F}, \subset_{\mathcal{F}})$ is a poset. ◇

Example 9.20.1 Let P be a nonempty subset of $\mathbb{N}$. The "divisibility" in P is defined as,

$$\leq_P \stackrel{\text{def}}{=} \{(a,b) \in P \times P \ : \ \exists\, q \in \mathbb{N},\ b = aq\}.$$

Then $(P, \leq_P)$ is a poset. ◇

Example 10.20.1 Hasse diagram

One may depict posets schematically usually called the *Hasse diagram* of the poset, which is a simple graph whose vertex set is the poset itself drawn in different levels in which we draw an edge uv *upwards* if $u \leq v$ (we sometimes use directed edges to emphasize the upward ordering). For instance, let the set P in Example 9.20.1 be the set of divisors of 30; i.e

$$P \stackrel{\text{def}}{=} \{1, 2, 3, 5, 6, 10, 15, 30\}.$$

Then the Hasse diagram of $(P, \leq_P)$ is the graph depicted in Figure 20.1. ◇

Definition 11.20.1 A *total order relation* or a *linear order relation* or a *total order* on a set X is a partial order on X in which any two members x and y of X are *comparable* in the sense that either $x \leq y$ or $y \leq x$ is true. ▶

A *totally ordered set* or a *linearly ordered set* is an ordered pair $(A, \leq)$ such that A is a nonempty set and $\leq$ is a total order relation on A. A totally ordered set is also called a *chain*.

Clearly, if $(X, \leq)$ is a totally ordered set and $Y \subseteq X$, then the induced partial order from X to Y is also a total order on Y called the *induced total order* on Y.

Definition 12.20.1 Let $(P, \leq)$ be a poset and B a subset of P.

i) An element $u \in P$ is said to be an *upper bound* of B (in P), if for every $b \in B$, $u \geq b$.

ii) An element $u_0 \in P$ is called the *least upper bound* or the *supremum* of B (in P), if u_0 is an upper bound of B and for any other upper bound of B such as u we have $u_0 \leq u$.

iii) A element $l \in P$ is a *lower bound* of B (in P), if for every $b \in B$, $v \leq b$.

iv) An element $v_0 \in P$ is the *greatest lower bound* or *infimum* of B (in P), if v_0 is a lower bound of B and for every other lower bound of B such as v, we have $v_0 \geq v$.

v) An element $m \in P$ is a *maximal* element of P, if for every $a \in P$, $a \geq m$ implies that $a = m$; i.e. no member of P is strictly greater than m.

vi) An element $m \in P$ is a *minimal* member of P, if for every $a \in P$, from $a \leq m$ it follows that $a = m$; i.e. no member of P is strictly smaller than m.

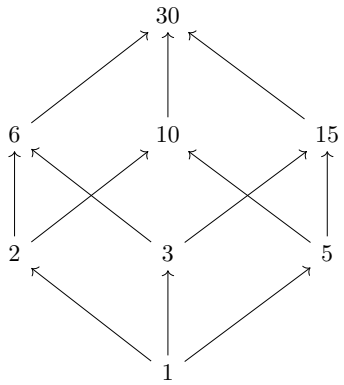

Figure 20.1 – A Hasse diagram (see Example 10.20.1).

DRAFT

vii) An element $m \in P$ is the *minimum* or *initial* or the *least* member of P, if for every $a \in P$, $m \leq a$.

viii) An element $m \in P$ is the *maximum* or *terminal* or the *greatest* member of P, if for every $a \in P$, $m \geq a$.

▶

Example 13.20.1

Consider the poset $(P \overset{\text{def}}{=} \{a, b, c, d, e\}, \leq)$ whose Hasse diagram is depicted in Figure 20.2. Then, for this poset,

- The element a is the *maximum* and a *maximal* element of P.
- The poset has no *minimum* element, however, d and e are *minimal* elements of P.
- The set $\{d, e\}$ is the set of *lower bounds* of the subset $\{a, b, c\}$.
- Since the set $\{d, e\}$ has no maximum element, the *infimum* of the subset $\{a, b, c\}$ does not exist, while its *supremum* exists and is equal to $a \in \{a, b, c\}$.
- The *supremum* of the subset $\{b, c\}$ exists and is equal to $a \notin \{b, c\}$.

◇

It is clear that if a subset B of P has a supremum (resp. infimum, maximum or minimum), then it is unique. The supremum (respectively, infimum) of a subset B (if it exists), is usually denoted by $\sup B$ (resp. $\inf B$). If B has an upper (resp. a lower) bound, then we say that B is *bounded above* (resp. *bounded below*). Also, B is called *bounded*, if it is both bounded above and below. If $\{x_i\}_{i \in I}$ is a collection of elements of a poset P which has a supremum (resp. an infimum) in P, then its supremum (resp. infimum) is represented by $\sup\limits_{i \in I} x_i$ or $\bigvee\limits_{i \in I} x_i$ (resp. $\inf\limits_{i \in I} x_i$ or $\bigwedge\limits_{i \in I} x_i$). Also, if $B \subseteq P$ has a supremum (resp. an infimum), then it is denoted by $\sup\limits_{b \in B} b$ or $\bigvee\limits_{b \in B} b$ (resp. $\inf\limits_{b \in B} b$ or $\bigwedge\limits_{b \in B} b$). Finally, if $\{a, b\}$ has a supremum (resp. an infimum), then it is usual to write $a \vee b \overset{\text{def}}{=} \sup\{a, b\}$(resp. $a \wedge b \overset{\text{def}}{=} \inf\{a, b\}$).

Definition 14.20.1 Let X and Y be two posets and $f : X \bullet\!\!\longrightarrow Y$ a map.

i) f is *increasing (resp. strictly increasing),* if

$$\forall\ a, b \in X, \quad a \geq b \Rightarrow f(a) \geq f(b).$$

$$(resp.\ \forall\ a, b \in X, \quad a > b \Rightarrow f(a) > f(b).)$$

ii) f is *decreasing (resp. strictly decreasing),* if

$$\forall\ a, b \in X, \quad a \leq b \Rightarrow f(a) \leq f(b).$$

$$(resp.\ \forall\ a, b \in X, \quad a < b \Rightarrow f(a) < f(b).)$$

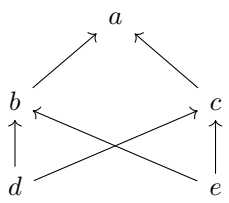

Figure 20.2 – The Hasse diagram of the poset $(\{a, b, c, d, e\}, \leq)$ (see Example 13.20.1).

DRAFT

iii) f is *order isomorphism* or briefly *isomorphism,* if f is increasing, one to one and onto.

iv) f is *dual order isomorphism* or briefly *dual isomorphism,* if f is decreasing, one to one and onto.

v) f is a *monomorphism,* if f is increasing and one to one.

vi) X is said to be *isomorphic (dual isomorphic)* to Y, if there is an isomorphism (dual isomoprphism) from X to Y.

▶

Proposition 15.20.1 *Let X, Y and Z be three posets.*

i) *If $f : X \bullet\!\!\longrightarrow Y$ is an isomorphism (resp. dual isomorphism), then f is strictly increasing (resp. strictly decreasing).*

ii) *Every poset X is isomorphic to itself. If X is isomorphic to Y, then Y is also isomorphic to X. If X is isomorphic to Y and Y is isomorphic to Z, then X is isomorphic to Z. Consequently, if $\{X_i\}_{i\in I}$ is a family of posets, then the following relation defined on the family is an equivalence relation.*

$$\forall\ i, j \in I, \quad X_i \ \mathcal{R}\ X_j \Leftrightarrow \textit{There is an isomorphism from } X_i \text{ to } X_j.$$

Thus, if X is isomorphic to Y, then Y is also isomorphic to X and in this case we say simply that X and Y are isomorphic.

Proposition 16.20.1 *Let X and Y be two posets, $f : X \bullet\!\!\longrightarrow Y$ an isomorphism, $g : X \bullet\!\!\longrightarrow Y$ a dual isomorphism and $\{x_i\}_{i\in I}$ a collection of elements of X.*

i) *A necessary and sufficient condition for $\bigvee_{i\in I} x_i$ (resp. $\bigwedge_{i\in I} x_i$) to exist in X is that $\bigvee_{i\in I} f(x_i)$ (resp. $\bigwedge_{i\in I} f(x_i)$) exists in Y and if this is the case, then*

$$f(\bigvee_{i\in I} x_i) = \bigvee_{i\in I} f(x_i).$$

$$(\textit{resp. } f(\bigwedge_{i\in I} x_i) = \bigwedge_{i\in I} f(x_i).)$$

In particular, if $a, b \in X$, then $f(a \wedge b) = f(a) \wedge f(b)$. (resp. $f(a \vee b) = f(a) \vee f(b)$.)

ii) *A necessary and sufficient condition for $\bigvee_{i\in I} x_i$ (resp. $\bigwedge_{i\in I} x_i$) to exist in X, is that $\bigwedge_{i\in I} g(x_i)$ (resp. $\bigvee_{i\in I} g(x_i)$) exist in Y and then*

$$g(\bigvee_{i\in I} x_i) = \bigwedge_{i\in I} g(x_i).$$

$$(\textit{resp. } g(\bigwedge_{i\in I} x_i) = \bigvee_{i\in I} g(x_i).)$$

In particular, if $a, b \in X$, then $g(a \vee b) = g(a) \wedge g(b)$. (resp. $g(a \wedge b) = g(a) \vee g(b)$.)

Proposition 17.20.1 *Let X and Y be two posets and $f : X \bullet\!\!\longrightarrow Y$ and $g : X \bullet\!\!\longrightarrow Y$ be isomorphism and dual isomorphism, respectively. Then,*

i) *a is a maximal (resp. minimal, maximum, infimum) element of X, if and only if $f(a)$ is a maximal (resp. minimal, maximum, infimum) element of Y.*

DRAFT

ii) *a is a maximal (resp. minimal, maximum, infimum) element of X, if and only if $g(a)$ is a minimal (resp. maximal, minimum, maximum) element of Y.*

Two important properties of $\mathbb{N}$, the set of natural numbers, is its *well-orderedness* and the validity of *induction principle* in its structure. The well-orderedness of $\mathbb{N}$ means that every nonempty subset of $\mathbb{N}$ has a least member. The induction principle in $\mathbb{N}$ says that if S is a subset of $\mathbb{N}$ such that $1 \in S$ and if $n \in S$ then $n+1 \in S$, then, $S = \mathbb{N}$. It follows immediately from this principle that if $p(n)$ is a property about a nondistinguished natural number n in such a way that $p(1)$ is true and the validity of $p(n)$ implies the correctness of $p(n+1)$, then $p(n)$ is true for all $n \in \mathbb{N}$. What follows is motivated by generalizing these concepts.

Definition 18.20.1 Let A be a poset. We say that A satisfies the *descending chain condition* or briefly, *DCC*, if every nonempty subset of A has a minimal member. A totally ordered set or a chain satisfying DCC is said to be a *well-ordered* set. ▶

If A satisfies DCC and $a \in A$, then the set $\{x \in A \ : \ x < a\}$ is called the *initial section* defined by a and is denoted by $s(a)$. When we speak about a section of A, or when we say that a set B is a section of A, our purpose is a section defined by a member $a \in A$.

Posets satisfying DCC have some properties similar to $\mathbb{N}$ making it possible to extend induction principle to a more general setting.

Theorem 19.20.1 (**The generalized induction principle**). *Let $(A, \leq)$ be a poset satisfying DCC and assume that $p(x)$ is a proposition defined for every $x \in A$. In addition, assume that*

i) *$p(x)$ is true for every minimal member of A.*

ii) *For every $a \in A$, the truth of $p(x)$ for all members of $s(a)$ implies the truth of $p(a)$.*

Then, $p(x)$ is true for all $x \in A$.

Note that Condition (i) automatically follows from Condition (ii), since if a is a minimal member of A, then $s(a) = \emptyset$ and there is no member $x \in s(a)$ for which $p(x)$ is false.

20.1.6 Algebraic Structures

Here we go through our first steps to introduce an abstract mathematical theory, which, inevitably, asks for an abstract language. The student who is not familiar with modern mathematics, not only may not be able to understand the importance of this *abstraction*, in particular in computer science, but also may find the new concepts and definitions quite hard to digest; however, it is well known that the idea of considering mathematical objects as sets with structures which satisfy some global properties, known as *axioms*, has deeply influenced the whole mathematics during the last century. We have decided to choose an approach along this line of development because we believe in its global advantages, although, we hope that, at the beginning, the student can overcome this rigidity of subjects by spending a good time on the examples and exercises.

Algebraic structures[3] are among the most popular mathematical structures, and maybe, besides their primitivity, one of the basic reasons for this is that they have been evolved from the ordinary *number systems* with their well–known operations such as *addition*, *subtraction* or *multiplication*. Strictly speaking, an algebraic structure is a nonempty set X along with a number of operations on it such that these operations satisfy some axioms. In this, the first thing which should be made clear is the concept of an *operation*.

Consider the set of *natural numbers*, $\mathbb{N}$, with addition and subtraction of numbers. Should we consider these two as operations on this set? Note that when we are talking about an operation on a set X, intuitively, we are talking about a black–box whose inputs and output are from the set X (see Figure 20.3). This simple observation has a number of important consequences.

The first of these is that for any set of inputs we should get an output which is in X. This is usually referred to as *well–definedness* or *closeness* of the operation. For instance, subtraction can not be considered as an operation on $\mathbb{N}$, since $1 - 2$ is not an element of $\mathbb{N}$.

Now if one tries to explain the above scenario mathematically, one obtains the following definition.

[3] Reference to the History and Kharazmi

DRAFT

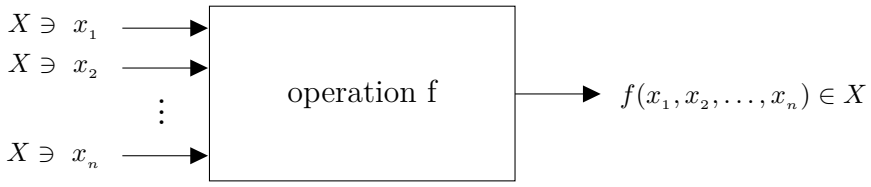

Figure 20.3 – An n–ary operation on the set X.

Definition 20.20.1 An *n-ary operation* ($n \geq 0$) on the nonempty set X is a map

$$f : X^n \longrightarrow X,$$

where each component of the domain of f is called an *operand* of f. Note that, 1-ary operations are usually called *unary* operations, while 2-ary operations are usually called *binary* operations. Also, by definition, a *nullary* (0-ary) operation on a nonempty set X is also defined, pathologically, as choosing a fixed element of X. ▶

The second observation is a matter of notation and is among the most basic reasons for further misunderstandings. We try to clarify it in the following example.

Example 21.20.1 Consider addition, $(+)$, as a binary operation on the set of natural numbers $\mathbb{N}$. Now, note that in our current language this is a map such as

$$+ : \mathbb{N} \times \mathbb{N} \bullet\!\!\longrightarrow \mathbb{N},$$

which means that in order to show $2 + 3 = 5$ we should write $+(2, 3) = 5$. This may seem to be absurd at first, however, when one considers n–ary operations for $n > 2$ then the new language shows its efficiency. It is also clear that $(+)$ has two operands with the same role since addition is a *commutative* operation on $\mathbb{N}$.
If we fix one operand of an n–ary operation when $n > 1$, then we obtain an $(n-1)$–ary operation, while the usual notation does not seem to be quite appropriate for these kind of manipulations. For instance, consider the operation of *addition by* 7 on $\mathbb{N}$ which is easily explained by the following map in our new language,

$$+(7, .) : \mathbb{N} \bullet\!\!\longrightarrow \mathbb{N}.$$

In this, our notation for the new operation is to put the fixed values in their own place. This shows that in order to compute the value of the new operation one can put the value of the operand in place of the dot and apply the old operation.
As one more example, let $f : \mathbb{N}^3 \longrightarrow \mathbb{N}$ be a 3–ary operation on natural numbers and assume that we want to consider the new 1–ary operation which can be obtained by fixing the values of the first and the third operands to 2 and 11 respectively. Then this new operation can be shown as follows,

$$f(2, ., 11) : \mathbb{N} \longrightarrow \mathbb{N}.$$

Throughout this book we may switch between these languages freely and we hope that it will cause no further ambiguity. ◇

The third observation is more fundamental and can be considered as one of the motivations for the whole abstract approach which comes in the sequel.

Example 22.20.1 Consider the set of *integers* $\mathbb{Z} \stackrel{\text{def}}{=} \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ with subtraction as an operation on it. What is the type of this operation?
Based on our intuition, we are accustomed to consider it as the following binary operation,

$$- : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z},$$

which sends (x, y) to $x - y$; although, in this approach we should be already familiar with rules such as $-(-y) = y$. Now the first question which comes to mind is "Why should such equations hold?"
This motivates the following reformulation which considers "$-$" as the following

DRAFT

1–ary operation,

$$- : \mathbb{Z} \longrightarrow \mathbb{Z},$$

which sends x to $-x$. Naturally, in this approach we shall interpret $x - y$ as $x + (-y)$. But this is actually an special kind of composition of these operations as maps and can be written in our new notation as

$$+(., -(.)) : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}.$$

◇

Strictly speaking, and *algebraic structure* is a set with a couple of operations on it that satisfy some properties (called axioms) themselves or in relation to each other. In what follows you will encounter some basic and fundamental algebraic structures as *monoids* and *lattices* , where we will discuss the whole thing once more in Section 20.2.2 from a more general viewpoint. The part of mathematics that studies algebras themselves (rather than specific examples, i.e. models) is called *universal algebra* in which one develops standard algebraic constructions as *subalgebras*, *quotient algebras*, as well as more sophisticated constructions and classifications (e.g. see []). In this book, we encounter *pre-automata* as very simple examples of algebras and we will use these techniques in this special case to study and characterize these simple computers as algebraic structures. ⟶ Sec. 7.2

In what follows, we briefly recall some basic properties of a couple of the most important algebraic structures in theory of computation, namely *monoids* and *lattices*.

Monoids and words

In this section we introduce *monoids* as one of the most basic algebraic structures, along with one the most important examples of which with a central role in theory of computation, namely the set of finite words constructed using a finite set of symbols.

Definition 23.20.1 A *monoid* $(M, e, *)$ is a nonempty set M along with a nullary operation $e \in M$ and a binary operation $(*)$ on M such that

M1) $\forall\ x, y, z \in G \quad x * (y * z) = (x * y) * z,$

M2) $\exists\ e \in G\ \ \forall\ x \in G \quad x * e = e * x = x,$

The element $e \in M$ is called the (twosided) *identity element* . A monoid $(M, *)$ is said to be *Abelian* or *commutative* if it satisfies the following extra property, → Exr. 20.3.7

M3) $\forall\ x, y \in G \quad x * y = y * x.$

The property (M1) is usually called the *associative law*. Note that one usually writes xy for $x * y$ if there is no ambiguity. A pair $(M, *)$ that only satisfies property (M1) is usually called a *semigroup*. ▶ → Exr. 20.3.8

Example 24.20.1 Some basic monoids

As some simple examples one can easily see that $(\mathbb{N}, 0, +)$, $(\mathbb{Q}, 0, +)$, $(\mathbb{R}, 0, +)$ and $(\mathbb{R}, 1, \times)$ are all examples of commutative monoids. ◇

Example 25.20.1 Free monoid of words

Let Σ be a finite set of symbols. A *sequence* of elements of Σ of length n is an ordered n-tuple $(w_1, w_2, \ldots, w_n) \in \Sigma^n$ of elements of Σ. Similarly, a *string* (sometimes called a *word*) of elements of Σ of length n is a ordered list of n symbols from Σ as $w_1 w_2 \ldots w_n$. It is clear that there is a one to one correspondence between *strings of length n* and *sequences of length n* of elements of Σ, since both sets are equivalent to the set of total functions from $\mathbb{N}_n$ to Σ. For this, we use the same notation Σ^n for both concepts.

Hence, one may define the set Σ^*, consisting of all finite strings whose symbols are chosen from Σ. In other words, define

$$\Sigma^* \stackrel{\text{def}}{=} \{w_1 w_2 \ldots w_n \ :\ n \in \mathbb{N} \text{ and } \forall\ i \in [\![1, n]\!], w_i \in \Sigma\} = \bigcup_{n \in \mathbb{N}} \Sigma^n.$$

DRAFT

In this setting, we emphasize that, the *length* of a word $w = w_1 w_2 \dots w_n$, denoted by $|w|$ is defined to be equal to n, when ϵ is the *null word* of length zero (i.e. $|\epsilon| = 0$). Also, for $\Upsilon \subseteq \Sigma$ we define $|w|_\Upsilon$ as

$$|w|_\Upsilon \stackrel{\text{def}}{=} |\{w_i \ : \ 1 \leq i \leq n \ \text{ and } \ w_i \in \Upsilon\}|, \quad \text{and} \quad |w|_a \stackrel{\text{def}}{=} |w|_{\{a\}}.$$

Moreover, we define $\Sigma^0 \stackrel{\text{def}}{=} \{\epsilon\}$ and Σ^+ to be the following set,

$$\Sigma^+ \stackrel{\text{def}}{=} \Sigma^* - \{\epsilon\} = \bigcup_{n \in \mathbb{N}^+} \Sigma^n.$$

Also, the *concatenation* of two words $w \in \Sigma^*$ and $z \in \Sigma^*$ is a binary operation on Σ^* defined as follows,

$$w.z \stackrel{\text{def}}{=} wz \in \Sigma^*.$$

It is easy to verify that for any finite set of symbols Σ, the algebraic structure $(\Sigma^*, \epsilon, .)$ consisting of the set of all finite words Σ^*, along with the null word ϵ and the concatenation operation is a monoid which is not commutative. This is also called the *free monoid* constructed (or generated) by Σ. ◇

Definition 26.20.1 Let Σ be a finite set of symbols, and consider the word $w = w_1 w_2 \dots w_n$ along with its corresponding function $\sigma_w : [\![1, n]\!] \bullet\!\!\longrightarrow \Sigma$. Then

- Any word corresponding to a restriction as $\sigma_w|_{[\![1,m]\!]}$ for some $1 \leq m \leq n$ is called a *prefix* of w.
- Any word corresponding to a restriction as $\sigma_w|_{[\![m,n]\!]}$ for some $1 \leq m \leq n$ is called a *suffix* of w.
- Any word corresponding to a restriction as $\sigma_w|_{[\![t,m]\!]}$ for some $1 \leq t \leq m \leq n$ is called a *infix* of w.

The sets of prefixes, suffixes and infixes of a sequence w are denoted by $\text{Prefix}(w)$, $\text{Suffix}(w)$ and $\text{Infix}(w)$, respectively.

Also, given a word $w = w_1 w_2 \dots w_n$, the *interval* centered at w_i of radius k, is defined to be the infix $w[i,k] \stackrel{\text{def}}{=} w_s \dots w_i \dots w_t$ where $s = \max(i-k, 1)$ and $t = \min(n, i+k)$. The notation $d_\Upsilon(w)$ stands for minimum of $|j - i - 1|$ where $i \neq j$, $w = w_1 w_2 \dots w_n$ and $(w_i, w_j) \subseteq \Upsilon^2$.

In this setting, the word w^R, defined as $w^R \stackrel{\text{def}}{=} w_n w_{n-1} \dots w_1$, is called the *reverse* of the word w, and it is easy to verify that for any two words u and w in Σ^* we have $(w^R)^R = w$ and $(uw)^R = w^R u^R$. ▶

It is easy to verify that Σ^* is a countable set. In what follows we consider some other important order relations on this set. → Exr. 20.3.9

Example 27.20.1 The prefix order on Σ^*

Given a finite set of symbols, Σ, the *prefix order*, $\preceq$, is defined on Σ^* as follows,

$$u \preceq w \quad \Leftrightarrow \quad [u \text{ is a prefix of } w].$$

Naturally, $\prec$ stands for the *strict order*, for which $u \prec w$ means that $u \preceq w$ and $u \neq w$. Clearly, $\prec$ is a partial order on Σ^* and introduces a poset structure on this set (see Figure 20.4 for the Hasse diagram). ◇

Example 28.20.1 The lexicographic order on Σ^*

Given a finite totally ordered set of symbols, $\Sigma = \{s_1, s_2, \dots, s_k\}$, with $s_1 < s_2 < \dots < s_k$, the *strict lexicographic order*, $\ll$, is defined on Σ^* as follows,

$$u \ll w \quad \Leftrightarrow \quad [(u \prec w) \text{ or } (u = v s_i z_1, \text{ and } w = v s_j z_2, \text{ and } s_i < s_j)].$$

Note that, in the lexicographic order either $u = w$ or $u \ll w$, and consequently, one deduces that this induces a total order structure on Σ^*. It is instructive to note that the lexicographic

DRAFT

order can be visualized as going "up" or "left to right" within the Hasse diagram of the prefix order depicted in Figure 20.4. ◇

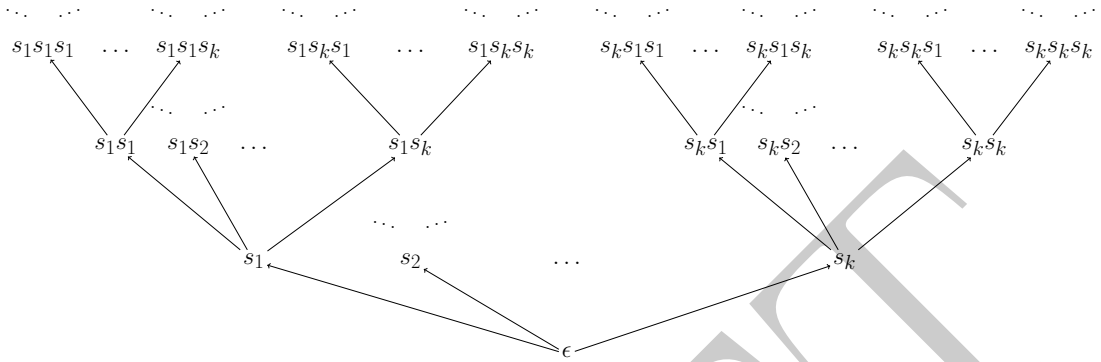

Figure 20.4 – The Hasse diagram of $(\{s_1, s_2, \ldots, s_k\}^*, \preceq)$ (see Example 27.20.1).

Example 29.20.1 Homomorphisms on words

Since Σ^* along with the concatenation operator is a monoid, one may think of homomorphisms of these algebraic structures and for two finite sets Σ and Γ define a map $\sigma : \Sigma^* \bullet\!\!\longrightarrow \Gamma^*$ to be a *homomorphism* if for any pair of words u and w in Σ^* the following equality holds, → Exr. 20.3.12

$$\sigma(uw) = \sigma(u)\sigma(w).$$

Note that, since Σ^* with the concatenation operator is a free monoid any map $f : \Sigma \bullet\!\!\longrightarrow \Gamma$ may be extended to a homomorphism $\sigma_f : \Sigma^* \bullet\!\!\longrightarrow \Gamma^*$ in a unique way. ◇ → Exr. 20.3.13

Example 30.20.1 Formal languages

Let Σ be a finite set of symbols. Then any subset of Σ^* as $L \subseteq \Sigma^*$ is said to be a *formal language* in Σ^*; while this choice of name is a reminiscent of the set of words of a natural language, say English language, in $\{a, b, \ldots, z\}^*$.

Within this setting, for two languages K and L in Σ^* the concatenation of K with L, denoted by KL, is defined as, → Exr. 20.3.8

$$KL \stackrel{\text{def}}{=} \{uv \ : \ u \in K \text{ and } v \in L\}.$$

Then, following similar nomenclature of Example 25.20.1, one may talk about the language L^n where $L^0 \stackrel{\text{def}}{=} \{\epsilon\}$. Also, we may define L^* and L^+ as

$$L^* \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}} L^n, \quad \text{and} \quad L^+ \stackrel{\text{def}}{=} \bigcup_{n\in\mathbb{N}^+} L^n.$$

Within the same spirit, a language L is said to be ϵ-free if $\epsilon \notin L$, and moreover, we define the reverse of a language L, denoted as L^R, as

$$L^R \stackrel{\text{def}}{=} \{w^R \ : \ w \in L\}.$$

Also, the *right quotient*, L/K (sometimes denoted as LK^{-1}), and the *left quotient*, $K\backslash L$ (sometimes denoted as $K^{-1}L$), are defined as follows, → Exr.20.3.10

$$L/K \stackrel{\text{def}}{=} \{w \in \Sigma^* \ : \ \exists\, u \in K, \quad wu \in L\} \quad \text{and} \quad K\backslash L \stackrel{\text{def}}{=} \{w \in \Sigma^* \ : \ \exists\, u \in K, \quad uw \in L\}.$$

When $K = \{x\}$, for simplicity, we write, L/x and $x\backslash L$ for $L/\{x\}$ and $\{x\}\backslash L$, respectively. ◇

DRAFT

Lattices

Lattices are posets that also can be defined as algebraic structures. Let us begin with a couple of definitions.

Definition 31.20.1
If $*$ is a binary operation on a nonempty set A, then

i) The operation $*$ is *idempotent*, if and only if $\forall\ a \in A, \quad a * a = a.$

ii) The operation $*$ is *commutative*, if and only if $\forall\ a, b \in A, \quad a * b = b * a.$

iii) The operation $*$ is *associative*, if and only if $\forall\ a, b, c \in A, \quad a * (b * c) = (a * b) * c.$

▶

Definition 32.20.1
A *semilattice* is a nonempty set A with a binary operation $*$ defined on it which is idempotent, commutative and associative. In this case, the semilattice is denoted by $(A, *)$.

A poset $(P, \leq)$ is said to be a *meet semilattice* (resp. *join semilattice*), if every two members of P have an infimum (resp. supremum) in P. A poset $(P, \leq)$ is said to be *complete,* if every nonempty subset of which has supremum and infimum. A poset $(P, \leq)$ is *conditionally complete,* if every nonempty bounded subset of which has supremum and infimum. ▶

If $(P, \leq)$ is a meet (resp. join) semilattice and $x, y \in P$, the infimum (supremum) of them in accordance with the previous notations is denoted by $x \wedge y$ (resp. $x \vee y$). If P is a meet (resp. join) semilattice, the binary operation $*$ on P can be defined as $a * b := a \wedge b$ ($a * b := a \vee b$) for all $a, b \in P$. It is convenience to note this operation with the same notation $\wedge$ (resp. $\vee$).

Proposition 33.20.1 *If $(P, \leq)$ is a meet (resp. join) semilattice, then the binary operation $\wedge$ (resp. $\vee$) assigning to each pair of members $a, b \in P$ their infimum (resp. supremum) is idempotent, commutative and associative. Thus, $(P, \wedge)$ (resp. $(P, \vee)$) is a semilattice.*

Proposition 34.20.1 *If $(P, \leq)$ is a meet (resp. join) semilattice, then for every $a, b \in P$*

$$a \leq b \Leftrightarrow a \wedge b = a,$$

$$(resp. \quad a \leq b \Leftrightarrow a \vee b = b).$$

The proposition 34.20.1 states in fact that the partial order relation $\leq$ on a meet (resp. join) semilattice can be formulated completely by the operation $\wedge$ (resp. $\vee$). The important fact is that the converse of this statement is also true; i.e. when a semilattice is given, it can be made into the structure of a meet or join semilattice.

Proposition 35.20.1 *Let $(A, *)$ be a semilattice. Define the relation $\leq_1$ on A as follows.*

$$\forall\ a, b \in A, \quad a \leq_1 b \Leftrightarrow a * b = a.$$

Then, $\leq_1$ is a partial ordering on A and $(A, \leq_1)$ is a meet semilattice in which $a \wedge b = a * b$. In the same mannar, if $(A, \circ)$ is a semilattice and we define the relarion $\leq_2$ on A as

$$\forall\ a, b \in A, \quad a \leq_2 b \Leftrightarrow a \circ b = b,$$

then $\leq_2$ is a partial order relation and $(A, \leq_2)$ is a join semilattice such that $a \vee b = a \circ b$.

Proof. Since $*$ is idempotent, for every $a \in A$ we have $a * a = a$ and so $a \leq_1 a$, i.e. $\leq_1$ is idempotent. Let $a, b \in A$, $a \leq_1 b$ and $b \leq_1 a$. Then, $a * b = a$ and $b * a = b$. Since $*$ is commutative, $a * b = b * a$ and so $a = b$, i.e. $\leq_1$ is antisymmetric. Assume that $a, b, c \in A$, $a \leq_1 b$ and $b \leq_1 c$. Then, $a * b = a$ and $b * c = b$. We infer that

$$a * c = (a * b) * c = a * (b * c) = a * b = a,$$

DRAFT

i.e. $a \leq_1 c$. Thus, $\leq_1$ is transitive and is a partial order relation on A. We now show that for every $a, b \in A$, $a \wedge b = a * b$. Since

$$(a * b) * a = a * (b * a) = a * (a * b) = (a * a) * b = a * b,$$

we have $(a * b) * a = a * b$ and therefore $a * b \leq_1 a$. By the same reason, $a * b \leq_1 b$. Suppose that $c \in A$ and $c \leq_1 a$ and $c \leq_1 b$. Then, $c * a = c$ and $c * b = c$. It follows that

$$c * (a * b) = (c * a) * b = c * b = c,$$

i.e. $c \leq_1 a * b$. In other words, $a * b$ is the same as $a \wedge b$.
It is proved by the same manner that $(A, \leq_2)$ is a join semilattice in which $a \vee b = a \circ b$ for all $a, b \in A$. □

Definition 36.20.1 A poset $(P, \leq)$ is said to be a *lattice,* if $(P, \leq)$ is simultaneously a meet and a join semilattice.

A lattice $(P, \leq)$ is said to be *distributive*, if

i) $\forall\ a, b, c \in P, \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$,

ii) $\forall\ a, b, c \in P, \quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

▶

Theorem 37.20.1 *If $(P, \leq)$ is a lattice, then the binary operations $\wedge$ and $\vee$ are idempotent, commutative and associative. In addition,* → Exr. 20.3.14

$$\forall\ a, b \in P, \quad a \wedge (a \vee b) = a \vee (a \wedge b) = a.$$

Conversely, let $(A, *, \circ)$ be a set with two binary operations $*$ and $\circ$ such that $(A, *)$ and $(A, \circ)$ are semilattices and also

$$\forall\ a, b \in A, \quad a * (a \circ b) = a \circ (a * b) = a.$$

Then, there is a partial order relation $\leq$ on A in such a way that $(A, \leq)$ is a lattice in which

$$\forall\ a, b \in A, \quad a \wedge b = a * b \text{ and } a \vee b = a \circ b.$$

Proof. The idempotency, commutativity and associativity of operations $\wedge$ and $\vee$ are the immediate consequenses of the definition of a lattice and proposition 33.20.1. Also, according to proposition 34.20.1, to prove $a \wedge (a \vee b) = a$ it sufices to show $a \leq a \vee b$ which is evident. By the same way, it is proved that $a \vee (a \wedge b) = a$, since $a \wedge b \leq a$.

Conversely, if $(A, *, \circ)$ satisfies the conditions stated in the theorem, then we define

$$\forall\ a, b \in A \quad a \leq_1 b \Leftrightarrow a * b = a.$$

Now, since $(A, *)$ is a semilattice, it follows at once from proposition 35.20.1 that $(A, \leq_1)$ is a meet semilattice and $a \wedge b = a * b$. Similarly, because $(A, \circ)$ is also a semilattice, by the same proposition, we conclude that if we define

$$\forall\ a, b \in A \quad a \leq_2 b \Leftrightarrow a \circ b = b,$$

then $(A, \leq_2)$ is a join semilattice and $a \vee b = a \circ b$.

To complete the proof, it is sufficient to prove that the relations $\leq_1$ and $\leq_2$ are in fact equal; i.e.

$$\forall\ a, b \in A \quad a \leq_1 b \Leftrightarrow a \leq_2 b.$$

In other words, we must show that $a * b = a \Leftrightarrow a \circ b = b$.
Let $a * b = a$. Then,

DRAFT

$$\begin{aligned} a \circ b &= (a * b) \circ b \\ &= b \circ (a * b) && \text{(commutativity of } \circ) \\ &= b \circ (b * a) && \text{(commutativity of } *) \\ &= b && \text{(since } \forall\, x, y \in A, \quad x \circ (x * y) = y). \end{aligned}$$

Conversely, if $a \circ b = b$, then by interchanging the rule of $*$ and $\circ$ in the above steps, it follows that $a * b = a$. □

Although it is true that a lattice may posses neither greatest nor smallest members; but if it has the former, it is usually denoted by 1 and if the later, by 0.

Definition 38.20.1 Let $(P, \leq)$ be a lattice with the least member 0 and the greatest member 1 and let a be a member of P. An element $b \in P$ is called a *complement* of a in P, if and only if

$$a \wedge b = 0 \text{ and } a \vee b = 1.$$

The lattice $(P, \leq)$ is called *complemented,* if every member from it has a complement. ▶

Proposition 39.20.1 *Statements* (i) *and* (ii) *in Definition* 36.20.1 *are equivalent.*

Proof. Let i be true and assume that a, b and c are three members of P. Then, replacing a, b and c in i by $a \vee b$, a and c respectively, we have

$$\begin{aligned} (a \vee b) \wedge (a \vee c) &= ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = (a \wedge (a \vee b)) \vee (c \wedge (a \vee b)) \\ &= a \vee (c \wedge (a \vee b)) = a \vee ((c \wedge a) \vee (c \wedge b)) = (a \vee (c \wedge a)) \vee (c \wedge b) \\ &= a \vee (c \wedge b) \end{aligned}$$

□

Definition 40.20.1 Boolean algebras A lattice $(P, \leq)$ is called a *Boolean algebra*, if it is complemented and distributive. ▶

Example 41.20.1 Let A be a nonempty set and $\mathcal{E}$ the collection of all equivalence relations on A. Then $\mathcal{E}$ can be given the structure of a poset by the inclusion relation as follows.

$$\forall\, R_1, R_2 \in \mathcal{E}, \quad R_1 \leq R_2 \Leftrightarrow R_1 \subseteq R_2.$$

The pair $(\mathcal{E}, \subseteq)$ is a complete lattice, since if one assumes that $\{R_\alpha\}_{\alpha \in \Delta}$ is a nonempty family of elements of $\mathcal{E}$, then

i) It is easy to see that $\bigcap_{\alpha \in \Delta} R_\alpha$ is also an equivalence relation on A and hence is in $\mathcal{E}$. Certainly

$$\bigwedge_{\alpha \in \Delta} R_\alpha = \bigcap_{\alpha \in \Delta} R_\alpha.$$

ii) We define a relation R on A such that for every $a, b \in A$, aRb, if and only if there exist a finite number of elements of $\{R_\alpha\}_{\alpha \in \Delta}$ such as $R_{\alpha_1}, \ldots, R_{\alpha_n}$ and elements $x_0, \ldots, x_n$ in A such that $x_0 = a$ and $x_n = b$ and for every $1 \leq i \leq n$, $x_{i-1} R_{\alpha_i} x_i$. It is easy to check that R is an equivalence relation on A containing all R_α. If S is also another equivalence relation on A containing all R_α and if $a, b \in A$, aRb, $R_{\alpha_1}, \ldots, R_{\alpha_n}$, $x_0, \ldots, x_n$ are as before, then since S contains each R_α, for every $1 \leq i \leq n$ we have $x_{i-1} S x_i$ and since S is transitive

$$x_0 S x_1,\ x_1 S x_2, \ldots, x_{n-1} S x_n \Rightarrow x_0 S x_n.$$

Thus, $(a, b) = (x_0, x_n) \in S$ i.e. $R \subseteq S$ and then

$$R = \bigvee_{\alpha \in \Delta} R_\alpha.$$

DRAFT

◇

Definition 42.20.1 Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two arbitrary collections of subsets of a set A. We say that $\mathcal{M}_1$ is *finer* than $\mathcal{M}_2$ or $\mathcal{M}_1$ is a *refinement* of $\mathcal{M}_2$ or $\mathcal{M}_2$ is *coarser* than $\mathcal{M}_1$, if

$$\forall\ X \in \mathcal{M}_1,\ \exists\ Y \in \mathcal{M}_2, \quad X \subseteq Y;$$

i.e. every element of $\mathcal{M}_1$ is contained in a member of $\mathcal{M}_2$. ▶

If $\mathcal{P}$ is the collection of all partitions of a set A, then $\mathcal{P}$ can be given the structure of a poset by the relation $\leq$ called the *refinement relation* as follows.

$$\forall\ \mathcal{M}_1, \mathcal{M}_2 \in \mathcal{P}, \quad \mathcal{M}_1 \leq \mathcal{M}_2 \Leftrightarrow \mathcal{M}_1 \text{is a refinement of } \mathcal{M}_2.$$

Proposition 43.20.1

i) *Let A be a nonempty set and $(\mathcal{E}, \subseteq)$ and $(\mathcal{P}, \leq)$ be respectively the poset of the family of all equivalence relations with the inclusion relation and the poset of the family of all partitions of A with the refinement relation. For each $R \in \mathcal{E}$ let $\mathcal{M}_R \in \mathcal{P}$ be the partition corresponding to R according to 4.20.1. Also, for each $\mathcal{M} \in \mathcal{P}$ let $R_{\mathcal{M}} \in \mathcal{E}$ be the equivalence relation corresponding to $\mathcal{M}$ according to 5.20.1. Then the map $\Phi : \mathcal{E} \bullet\!\!\longrightarrow \mathcal{P}$ which is defined as $\Phi(R) = \mathcal{M}_R$, is a dual isomorphism from $\mathcal{E}$ to $\mathcal{P}$. Also, the map $\Psi : \mathcal{P} \bullet\!\!\longrightarrow \mathcal{E}$ defined as $\Psi(\mathcal{M}) = R_{\mathcal{M}}$ is a dual isomorphism from $\mathcal{P}$ to $\mathcal{E}$ and Φ and Ψ are the converse of each other.*

ii) *$(\mathcal{P}, \leq)$ is a complete lattice.*

20.1.7 Closure operators and Moore families

Definition 44.20.1 Let $(P, \leq)$ be a poset.

i) A map $f : P \bullet\!\!\longrightarrow P$ is said to be a *closure operator* on P, if

C1) $\forall\ \{a, b\} \subseteq P, \quad a \leq b \Rightarrow f(a) \leq f(b)$ (i.e. f is increasing),
C2) $\forall\ a \in P, \quad a \leq f(a)$,
C3) $\forall\ a \in P, \quad f(f(a)) = f(a)$.

ii) An element $a \in P$ is said to be a *closed* element of f, if $f(a) = a$.

- A closure operator on the opposite poset $(P, \geq)$ is called an *interior operator* on $(P, \leq)$.

▶

If f is a closure operator on a poset P and C the collection of the closed elements of P, then C with the induced partial ordering imposed by P, becomes a poset. If A is a subset of C, then $\inf_C A$ and $\sup_C A$ subject to existence, can be found from $\inf_P A$ and $\sup_P A$.

Proposition 45.20.1 *Let $(P, \leq)$ be a poset, f a closure operator on P, and C the collection of closed elements of P with and $\emptyset \neq A \subseteq C$.*

i) *An element $b \in P$ is closed under f, if and only if there is an $a \in P$ with $f(a) = b$; in other words, $C = f(P)$.*

ii) *A necessary and sufficient condition for $\inf_C A$ to exist, is that $\inf_P A$ exists and when this is the case, we have*

$$\inf_P A = \inf_C A \in C.$$

Thus, the infimum of a collection of closed elements is itself closed.

DRAFT

iii) *If* $\sup_P A$ *exists, then* $\sup_C A$ *also exists and then*

$$\sup_C A = f(\sup_P A).$$

Proof. i) This is clear by definitions.

ii) Let $\inf_P A$ exist and set $a = \inf_P A$. In order to prove $a = \inf_C A$ it is enough to show that $a \in C$ i.e. $f(a) = a$. Since $a \leq f(a)$, we have to prove that $f(a) \leq a$ and since a is the infimum of A in P, it suffices to show that $f(a)$ is also a lower bound for A in P. If $b \in A$, it is clear that $b \geq a$ and since f is increasing, $f(b) \geq f(a)$. But, $b \in C$ and so $f(b) = b$ and $b \geq f(a)$. Therefore, $f(a)$ is a lower bound for A in P and $f(a) \leq a$.

Conversely, if $a = \inf_C A \in C$ exists, then a is clearly a lower bound for A in P. Now, assume that $m \in P$ and for each $n \in A$, $m \leq n$. Then $f(m) \leq f(n)$. Since $n \in A \subseteq C$, $f(n) = n$ and thus $f(m) \leq n$. By Part (i), $f(m)$ is in C and therefore is a lower bound for A in C. By definition, $f(m) \leq a = \inf_C A$. Hence, $m \leq f(m) \leq a$ and $m \leq a$, and consequently, a is in fact the infimum of A in P and $a = \inf_P A = \inf_C A$.

iii) Assume that $\sup_P A$ exists and $a = \sup_P A$. For each $b \in A$, we have $b \leq a$. Thus, $f(b) \leq f(a)$ and since $f(b) = b$, we have $b \leq f(a)$. By Part (i), $f(a) \in C$. So, $f(a)$ is an upper bound for A in C. Now, if $m \in A$ and m is an upper bound for A in C, m is also an upper bound for a in P, and therefore, $m \geq a = \sup_P A$. Hence, $f(m) \geq f(a)$, and since $m \in A \subseteq C$, $m = f(m) \geq f(a)$ i.e. $f(a) \in C$ is the least upper bound for A in C. Thus, $\sup_C A = f(a) = f(\sup_P A)$.

□

Theorem 46.20.1 *Let P be a complete lattice, f a closure operator on P and C the family of closed elements of P. Then C with the induced partial ordering, is also a complete lattice i.e. the collection of closed elements of a complete lattice under a closure operator forms a complete lattice.*

Definition 47.20.1 Let P be a complete lattice with the greatest element $1 \in P$. A subset M of P is said to be a *Moore family* of elements of P, if M is closed under taking arbitrary infimums i.e. if $\{x_i\}_{i \in I}$ is an arbitrary collection of elements of M, then $\bigwedge_{i \in I} x_i \in M$ (note that the infimum is taken in P). ▶

Note that if we choose I to be the empty family, then it follows from the definition of infimum that $\bigwedge_{i \in I} x_i = 1$ and thus $1 \in M$ i.e. any Moore family of elements of a complete lattice automatically contains the greatest element of the lattice.

Proposition 48.20.1

i) *Let $(P, \leq)$ be a poset and C the collection of all closure operators on P. Then C with the ordering relation $\leq_1$ defined as follows is a poset.*

$$\forall\ \phi, \psi \in \mathcal{C}, \quad (\phi \leq_1 \psi \Leftrightarrow (\forall\ a \in P, \quad \phi(a) \leq \psi(a))).$$

In fact, if we consider P^P with the pointwise ordering or componentwise order relation, then $\leq_1$ is the same as the induced partial ordering imposed from P^P on $\mathcal{C}$.

ii) *Suppose that P is a complete lattice and $\mathcal{M}$ is the family of all Moore families of elements of P. Then, $\mathcal{M}$ with the inclusion relation $\subseteq$ becomes a poset $(\mathcal{M}, \subseteq)$.*

Theorem 49.20.1 *Let P be a complete lattice and $(\mathcal{C}, \leq_1)$ and $(\mathcal{M}, \subseteq)$ be respectively the collection of all closure operators on P and the family of all Moore families of elements of P with the partial orderings defined in Proposition 48.20.1.*

DRAFT

i) *If* $\phi \in \mathcal{C}$ *and* $M_{_\phi} \overset{\text{def}}{=} \{a \in P \quad : \quad \phi(a) = a\}$, *then* $M_{_\phi} \in \mathcal{M}$.

ii) *Let* $M \in \mathcal{M}$ *and define the map* $\psi_{_M} : P \bullet\!\!\longrightarrow P$ *as follows.*

$$\forall\ a \in P, \quad \psi_{_M}(a) \overset{\text{def}}{=} \inf\{x \in M \quad : \quad x \geq a\}.$$

Then $\psi_{_M} \in \mathcal{C}$.

iii) *The map* $\Phi : \mathcal{C} \bullet\!\!\longrightarrow \mathcal{M}$ *defined by the formula* $\Phi(\phi) = M_{_\phi}$ *is a dual isomorphism from* $\mathcal{C}$ *to* $\mathcal{M}$. *Also, the map* $\Psi : \mathcal{M} \bullet\!\!\longrightarrow \mathcal{C}$ *defined as* $\Psi(M) = \psi_{_M}$ *is a dual isomorphism from* $\mathcal{M}$ *to* $\mathcal{C}$ *and* Φ *and* Ψ *are the converse of each other.*

Corollary 50.20.1

i) *If* P *is a complete lattice and* ϕ *a closure operator on* P, *then the collection of those elements of* P *which are closed under* ϕ *forms a Moore family of elements of* P.

ii) *If* P *is a complete lattice and* M *a Moore family of elements of* P, *then there is one and only one closure operator* ϕ *on* P *such that* M *is exactly the collection of closed elements of* P *under* ϕ.

iii) *If* P *is a complete lattice and* M *a Moore family of elements of* P, *then* M *with the induced partial ordering from* P *is a complete lattice such that if* A *is a subset of* M, *then*

$$\inf_{_M} A = \inf_{_P} A,$$

$$\sup_{_M} A = \inf_{_P}\{x \in M \quad : \quad x \geq \sup_{_P} A\}.$$

In particular, if f *is a closure operator on the complete lattice* P *and* C *is the collection of closed members of* P *under* f, *then*

$$\forall\ a \in P, \quad f(a) = \inf_{_P}\{x \in C \quad : \quad x \geq a\}.$$

If P *is a complete lattice and* ϕ *a closure operator on* P, *then the collection of those elements of* P *which are closed under* ϕ *forms a Moore family of elements of* P.

Example 51.20.1 Let X be a nonempty set, $(\mathcal{P}(X), \leq)$ the power set of X with the inclusion relation and $\mathcal{M}_{_0}$ a Moore family of elements of X (in this case, we say that $\mathcal{M}_{_0}$ is a Moore family of subsets of X). Then $(\mathcal{M}_{_0}, \subseteq)$ is a complete lattice, such that for every nonempty subset $\mathcal{A}$ of $\mathcal{M}_{_0}$ we have

$$\inf_{_{\mathcal{M}_{_0}}} \mathcal{A} = \bigcap_{_{a \in \mathcal{A}}} A;$$

$$\sup_{_{\mathcal{M}_{_0}}} \mathcal{A} = \bigcap_{_{B \in \mathcal{P}(X)}} \{B \in \mathcal{M}_{_0} \quad : \quad B \supseteq \bigcup_{_{A \in \mathcal{A}}} A\}.$$

◇

To see that how the machinery of closure operators and Moore families may prove to be useful, assume that you are interested in some specific subsets of a universal set U that satisfy some property P. In that case, if the collection of subsets having property P is a Moore family then you may be sure that property P is essentially a "closeness" property and you are able to talk about the closure of a subset $A \subseteq U$ with respect to property P which can be described as the smallest subset having property P and containing A. Note that this closure of A is guaranteed to exist by the Moore family property and can be expressed as the intersection of all subsets of U that contain A and satisfy P at the same time.

20.1.8 Graphs

Throughout this section we recall some basic definitions and concepts from graph theory. For more details and deeper facts the interested reader may consult the existing literature (e.g. see []).

DRAFT

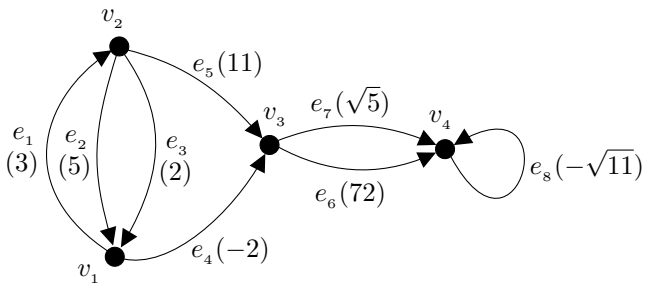

Figure 20.5 – A labeled multigraph $G(V, E, +, -, \mathbb{R})$ (see Example 53.20.1).

Definition 52.20.1 Variants of graphs

A labeled multigraph $G = (V, E, +, -, \ell)$ with labels from the set L, consists of a nonempty set of *vertices*, a set of *edges*, a function $+ : E \bullet\!\!\longrightarrow V$ that maps an edge $e \in E$ to its *terminal vertex* e^+, and similarly a function $- : E \bullet\!\!\longrightarrow V$ that maps an edge $e \in E$ to its *initial vertex* e^-, along with a *labeling map* $\ell : E \bullet\!\!\longrightarrow L$. Given a labeled multigraph $G = (V, E, +, -, \ell)$, the corresponding *base multigraph*, $G = (V, E, +, -)$, is a multigraph structure where we forget about the labels. This unlabeled structure is sometimes referred to as *an unweighted multigraphs*.

Since the maps $(-)$ and $(+)$ induce a direction on each edge, in general, a multigraph is a *directed graph* , meaning that the graph structure constitutes of directed edges. If a labeled multigraph $G = (V, E, +, -, \ell)$ satisfies the following conditions then G is said to be a *simple labeled graph* ,

SG1) $\forall\ \{u, v\} \subseteq V$, $\big([\exists!\ e_1, e_1^- = u \text{ and } e_1^+ = v] \text{ and } [\exists!\ e_2, e_2^- = v \text{ and } e_2^+ = u]\big)$, with $\ell(e_1) = \ell(e_2)$,

SG2) For any edge $e \in E$ we have $e^+ \neq e^-$.

Clearly, for simple graphs, for any pair of vertices $\{u, v\} \subseteq V$, there exists a unique pair of edges with opposite directions between u and v with the same label. Hence, since there are no *loops* (i.e. an edge e with $e^+ = e^-$), one may identify these pair of edges with an *undirected edge* $e \overset{\text{def}}{=} \{u, v\}$, sometimes written as uv for simplicity, with the same labeling. We may just talk about a *graph* G when the rest of the structure is clear from the context.

For any vertex $v \in V(G)$, the *out-neighborhood* of v is defined as

$$N_G^+(v) \overset{\text{def}}{=} \{u \in V \ :\ \exists\ e \in E(G)\ \ e^- = v,\ e^+ = u\}.$$

Similarly, the *in-neighborhood* of v is defined as

$$N_G^-(v) \overset{\text{def}}{=} \{u \in V \ :\ \exists\ e \in E(G)\ \ e^+ = v,\ e^- = u\},$$

and the *neighborhood* of v in G, $N_G(v)$, is defined as the union $N_G^-(v) \cup N_G^+(v)$. The concepts *in-degree*, $d_G^-(v)$, and *out-degree*, $d_G^+(v)$, of a vertex v are defined as $|N_G^-(v)|$ and $|N_G^+(v)|$, respectively.

The concepts of the *neighborhood*, and the *degree* of a vertex v, for a simple graph G, are defined *mutatis mutandis*. Also, we may exclude the subscript when the graph is clear from the context, ▶

Example 53.20.1

The graph depicted in Figure 20.5 shows a multigraph on 4 vertices in $V \overset{\text{def}}{=} \{v_1, v_2, v_3, v_4\}$ and 8 edges in $E \overset{\text{def}}{=} \{e_1, e_2, e_3, e_4, e_5, e_6, e_7, e_8\}$, and the labeling map $\ell : E \bullet\!\!\longrightarrow \mathbb{R}$ whose values appear in parentheses next to the edge name. For instance, in this setting, we have

$$e_8^- = e_8^+ = v_4, \quad e_1^- = e_2^+ = e_3^+ = v_1, \quad \text{and} \quad \ell(e_7) = \sqrt{5}.$$

Also, Figure 20.6 shows a simple graph and it corresponding symmetric multigraph. Note that,

DRAFT

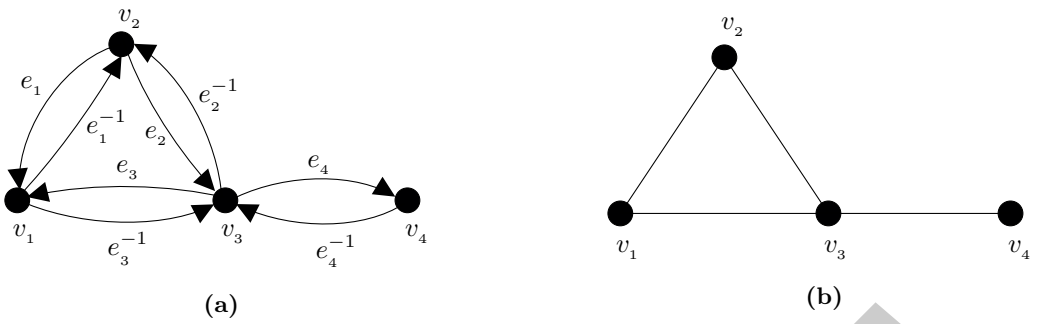

Figure 20.6 – A simple graph and its corresponding multigraph (see Example 53.20.1).

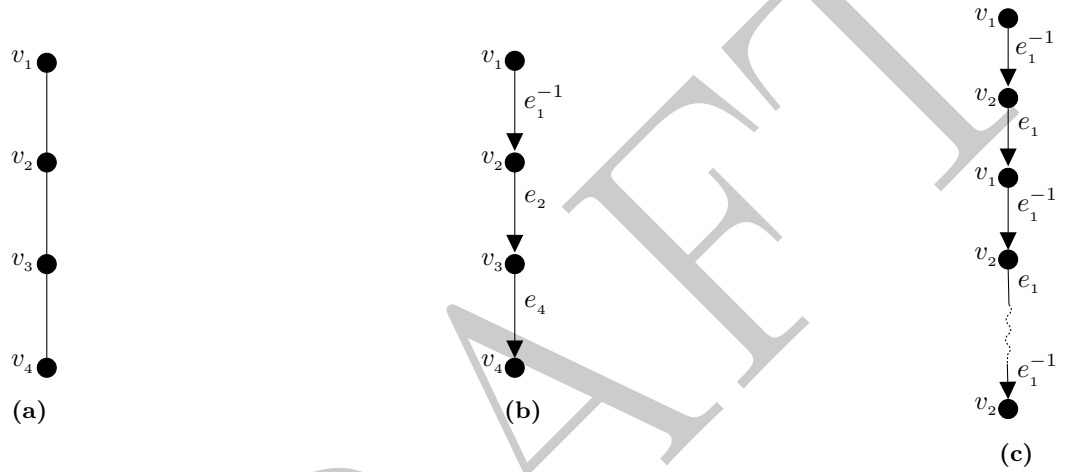

Figure 20.7 – Some examples of paths (see Example 55.20.1).

for this graph, one may refer to the *simple edge* v_1v_3 which is essentially the same as v_3v_1 since both refer to the set $\{v_1, v_3\}$ which is corresponding to the pair of edges $\{e_3, e_3^{-1}\}$. ◇

Definition 54.20.1 Walks, paths and cycles

A string in $(V \cup E)^*$ of the form $v_1e_2v_3e_4 \dots e_{2n}v_{2n+1}$ where odd symbols are vertices and even symbols are edges is called a *walk* of length n with the starting vertex v_1 and the ending vertex v_{2n+1}, if

$$\forall\, 1 \leq i \leq n, \quad e_{2i}^- = v_{2i-1} \text{ and } e_{2i}^+ = v_{2i+1}.$$

A *path* is a walk in which all vertices are distinct. A *cycle* is a walk in which all vertices are distinct except $v_1 = v_{2n+1}$. ▶

Example 55.20.1

Figure 20.7(a) shows a simple path of length 3, while one may also consider this path as a path which is a subgraph of the graph depicted in Figure 20.6(b). Similarly, Figure 20.7(b) shows a directed path of length 3, while one may also consider this path as a path which is a subgraph of the multigraph depicted in Figure 20.6(a).

Figure 20.7(c) shows an infinite directed walk on the two edges e_1 and e_1^{-1}, between vertices v_1 and v_2. ◇

Definition 56.20.1 Connected graphs and trees

Given a graph G, one may define the relation $\sim$ on the set of vertices as follows,

$$u \sim v \quad \Leftrightarrow \quad \text{(there exists a walk starting at } u \text{ and ending at } v\text{)}.$$

It is easy to verify that $\sim$ is an equivalence relation, and one may talk about the equivalence

DRAFT

classes which are called *connected components*. A graph is said to be a *connected graph* if the relation $\sim$ induces only one equivalence class on the set of vertices. A graph that do not contain any cycle is called a *forest*. A connected forest is called a *tree*.

A *rooted tree* (T, r) is a tree T, along with a distinguished vertex r of it, called *the root* (see Figure 20.8). If (T, r) is either a simple rooted tree or a directed rooted tree in which the direction of edges are always away from the root, then one may talk about the *distance* of a vertex from the root. In this way, one may draw the root at, say, level zero, and each other vertex at the level corresponding to its distance from the root. In this way, vertices at the same level are not connected to each other and edges are always drawn between two consecutive level (say from the upper level to the lower level). ▶

→ Exr. 20.3.16

Example 57.20.1

Figure 20.8 shows a couple of directed trees. Note that, Figure 20.8(a) can be regarded as a finite rooted tree with the root v_1, where other vertices appear at the first and the second level. Also, Figure 20.8(b) shows an infinite rooted tree with the root u_1, in which there exists an infinite path $u_1 u_6 u_7 u_8 \cdots$.

◇

DRAFT

Figure 20.8 – A couple of trees (see Example 57.20.1).