CHAPTER 2

SETS, RELATIONS, ORDERS AND FIELDS

2.1. Sets and functions

2.1.1. Sets. — A *set* is a collection of objects which are called *elements.*
Write
$$s \in S \text{ if } s \text{ is an element of the set } S.$$

- The *empty set* $\emptyset$ is the set with no elements.
- A *subset* T of a set S is a set T such that if $t \in T$ then $t \in S$.

Write
$$\begin{aligned} &T \subseteq S \text{ if } T \text{ is a subset of } S, \text{ and} \\ &T = S \text{ if the set } T \text{ is equal to the set } S. \end{aligned}$$

Let S and T be sets.

- The *union of* S *and* T is the set $S \cup T$ of all u such that $u \in S$ or $u \in T$,
$$S \cup T = \{u \mid u \in S \text{ or } u \in T\}.$$
- The *intersection of* S *and* T is the set $S \cup T$ of all u such that $u \in S$ and $u \in T$,
$$S \cap T = \{u \mid u \in S \text{ and } u \in T\}.$$
- The *product* S *and* T is the set $S \times T$ of all ordered pairs (s,t) where $s \in S$ and $t \in T$,
$$S \times T = \{(s,t) \mid s \in S \text{ and } t \in T\}.$$

The sets S and T are *disjoint* if $S \cap T = \emptyset$.
The set S is a *proper subset* of T if $S \subseteq T$ and $S \neq T$.

2.1.2. Functions. — Functions are for comparing sets.

Let S and T be sets. A *function from* S *to* T is a subset $\Gamma_f \subseteq S \times T$ such that
$$\text{if } s \in S \quad \text{then} \quad \text{there exists a unique } t \in T \text{ such that } (s,t) \in \Gamma_f.$$

Write
$$\Gamma_f = \{(s, f(s)) \mid s \in S\}$$

Notes of Arun Ram 5 August 2020

so that the function Γ_f can be expressed as

$$\text{an ``assignment''} \qquad \begin{array}{rccc} f\colon & S & \to & T \\ & s & \mapsto & f(s) \end{array}$$

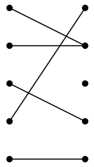
which must satisfy

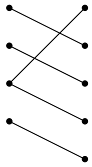
(a) If $s \in S$ then $f(s) \in T$, and
(b) If $s_1, s_2 \in S$ and $s_1 = s_2$ then $f(s_1) = f(s_2)$.

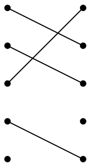
Let S and T be sets.

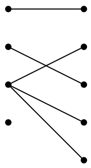
- Two functions $f\colon S \to T$ and $g\colon S \to T$ are *equal* if they satisfy
$$\text{if } s \in S \quad \text{then} \quad f(s) = g(s).$$
- A function $f\colon S \to T$ is *injective* if f satisfies the condition
$$\text{if } s_1, s_2 \in S \text{ and } f(s_1) = f(s_2) \quad \text{then} \quad s_1 = s_2.$$
- A function $f\colon S \to T$ is *surjective* if f satisfies the condition
$$\text{if } t \in T \quad \text{then} \quad \text{there exists } s \in S \text{ such that } f(s) = t.$$
- A function $f\colon S \to T$ is *bijective* if f is both injective and surjective.

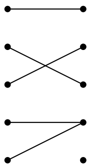
Examples. It is useful to visualize a function $f\colon S \to T$ as a graph with edges $(s, f(s))$ connecting elements $s \in S$ and $f(s) \in T$. With this in mind the following are examples

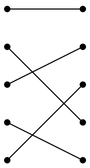

(a) a function


(b) not a function


(c) not a function


(c) an injective function


(d) a surjective function


(e) a bijective function

In these pictures the elements of the left column are the elements of the set S and the elements of the right column are the elements of the set T. In order to be a function the graph must have exactly one edge adjacent to each point in S. The function is injective if there is at most one edge adjacent to each point in T. The function is surjective if there is at least one edge adjacent to each point in T.

2.1.3. Composition of functions. — Let $f\colon S \to T$ and $g\colon T \to U$ be functions. The *composition* of f and g is the function

$$g \circ f \quad \text{given by} \quad \begin{array}{rccc} g \circ f\colon & S & \to & U \\ & s & \mapsto & g(f(s)) \end{array}$$

Let S be a set. The *identity map on S* is the function given by

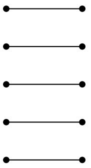
$$\begin{array}{rccc} \mathrm{id}_S\colon & S & \to & S \\ & s & \mapsto & s \end{array}$$

Let $f\colon S \to T$ be a function. The *inverse function to f* is a function

$$f^{-1}\colon T \to S \qquad \text{such that} \qquad f \circ f^{-1} = \mathrm{id}_T \quad \text{and} \quad f^{-1} \circ f = \mathrm{id}_S.$$

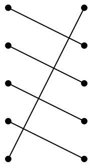
Theorem 2.1.1. — *Let $f\colon S \to T$ be a function. An inverse function to f exists if and only if f is bijective.*

Representing functions as graphs, the identity function id_S looks like

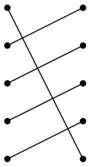


(a) the identity function id_S

In the pictures below, if the left graph is a pictorial representation of a function $f\colon S \to T$ then the inverse function to f, $f^{-1}\colon T \to S$, is represented by the graph on the right; the graph for f^{-1} is the mirror-image of the graph for f.

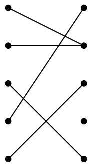


(b) the function f

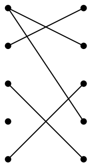


(c) the function f^{-1}

Graph (d) below, represents a function $g\colon S \to T$ which is not bijective. The inverse function to g does not exist in this case: the graph (e) of a possible candidate, is not the graph of a function.



(d) the function g



(e) not a function

2.1.4. Cardinality. — Let S and T be sets. The sets *S and T are isomorphic*, or *have the same cardinality*

$$\text{if there is a bijective function} \quad \varphi\colon S \to T.$$

Write $\mathrm{Card}(S) = \mathrm{Card}(T)$ if S and T have the same cardinality.

Notation: Let S be a set. Write

$$\mathrm{Card}(S) = \begin{cases} 0, & \text{if } S = \emptyset, \\ n, & \text{if } \mathrm{Card}(S) = \mathrm{Card}(\{1, 2, \ldots, n\}), \\ \infty, & \text{otherwise.} \end{cases}$$

Note that even in the cases where $\mathrm{Card}(S) = \infty$ and $\mathrm{Card}(T) = \infty$ it may be that $\mathrm{Card}(S) \neq \mathrm{Card}(T)$.

Let S be a set.

- The set S is *finite* if $\mathrm{Card}(S) \neq \infty$.
- The set S is *infinite* if $\mathrm{Card}(S)$ is not finite.

- The set S is *countable* if $\mathrm{Card}(S) = \mathrm{Card}(\mathbb{Z}_{>0})$.

Let $\mathcal{S}et$ be the set of sets. Define a relation $\sim$ on $\mathcal{S}et$ by

$$X \sim Y \qquad \text{if there exists a bijection } f\colon X \to Y.$$

The relation $\sim$ is an equivalence relation and $\mathrm{Card}(X)$ is the equivalence class of X. The set of *ordinals* is the set of equivalence classes of $\sim$,

$$\mathcal{O}rd = \{\mathrm{Card}(X) \mid X \in \mathcal{S}et\}.$$

Theorem 2.1.2. — *Define a relation $\preceq$ on $\mathcal{S}et$ by*

$$X \preceq Y \qquad \textit{if there exists an injection } f\colon X \to Y.$$

(a) *The relation $\preceq$ on $\mathcal{S}et$ gives a well defined relation $\leqslant$ on $\mathcal{O}rd$,*

$$\mathrm{Card}(X) \leqslant \mathrm{Card}(Y) \quad \textit{if there exists an injection } f\colon X \to Y,$$

where $X \in \mathrm{Card}(X)$ and $Y \in \mathrm{Card}(Y)$.
(b) *The relation $\leqslant$ is a partial order on $\mathcal{O}rd$.*

2.2. Relations, equivalence relations and partitions

Let S be a set.

- A *relation $\sim$ on S* is a subset $R_\sim$ of $S \times S$. Write $s_1 \sim s_2$ if the pair (s_1, s_2) is in the subset $R_\sim$ so that

$$R_\sim = \{(s_1, s_2) \in S \times S \mid s_1 \sim s_2\}.$$

- An *equivalence relation* on S is a relation $\sim$ on S such that
  (a) if $s \in S$ then $s \sim s$,
  (b) if $s_1, s_2 \in S$ and $s_1 \sim s_2$ then $s_2 \sim s_1$,
  (c) if $s_1, s_2, s_3 \in S$ and $s_1 \sim s_2$ and $s_2 \sim s_3$ then $s_1 \sim s_3$.

Let $\sim$ be an equivalence relation on a set S and let $s \in S$. The *equivalence class of s* is the set

$$[s] = \{t \in S \mid t \sim s\}.$$

A *partition of a set S* is a collection $\mathcal{P}$ of subsets of S such that
(a) If $s \in S$ then there exists $P \in \mathcal{P}$ such that $s \in P$, and
(b) If $P_1, P_2 \in \mathcal{P}$ and $P_1 \cap P_2 \neq \emptyset$ then $P_1 = P_2$.

Theorem 2.2.1. —
(a) *If S is a set and let $\sim$ be an equivalence relation on S then*

$$\textit{the set of equivalence classes of} \quad \sim \quad \textit{is a partition of } S.$$

(b) *If S is a set and $\mathcal{P}$ is a partition of S then*

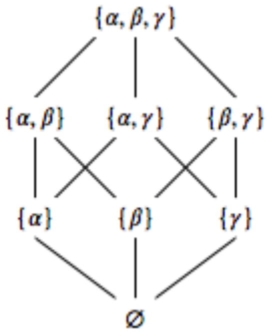
$$\textit{the relation defined by} \qquad s \sim t \quad \textit{if } s \textit{ and } t \textit{ are in the same } P \in \mathcal{P}$$

is an equivalence relation on S.

2.3. Partially ordered sets

Let S be a set.

- A *partial order* on S is a relation $\leqslant$ on S such that
  (a) If $x \in A$ then $x \leqslant x$,
  (b) If $x, y, z \in S$ and $x \leqslant y$ and $y \leqslant z$ then $x \leqslant z$, and
  (c) If $x, y \in S$ and $x \leqslant y$ and $y \leqslant x$ then $x = y$.
- A *total order* on S is a partial order $\leqslant$ such that
  (d) If $x, y \in S$ then $x \leqslant y$ or $y \leqslant x$.
- A *partially ordered set*, or *poset*, is a set S with a partial order $\leqslant$ on S.
- A *totally ordered set* is a set S with a total order $\leqslant$ on S.



The poset of subsets of $\{\alpha, \beta, \gamma\}$ with inclusion as $\leqslant$

Let S be a poset. Write

$$x < y \quad \text{if} \quad x \leqslant y \text{ and } x \neq y.$$

- The *Hasse diagram* of S is the graph with vertices S and directed edges given by

$$x \to y \qquad \text{if } x \leqslant y.$$

- A *lower order ideal of* S is a subset E of S such that

$$\text{if } y \in E \text{ and } x \in S \text{ and } x \leqslant y \quad \text{then} \quad x \in E.$$

- The *intervals in* S are the sets

$$\begin{array}{ll} S_{[a,b]} = \{x \in S \mid a \leqslant x \leqslant b\} & S_{(a,b)} = \{x \in S \mid a < x < b\} \\ S_{[a,b)} = \{x \in S \mid a \leqslant x < b\} & S_{(a,b]} = \{x \in S \mid a < x \leqslant b\} \\ S_{(-\infty,b]} = \{x \in S \mid x \leqslant b\} & S_{[a,\infty)} = \{x \in S \mid a \leqslant x\} \\ S_{(-\infty,b)} = \{x \in S \mid x < b\} & S_{(a,\infty)} = \{x \in S \mid a < x\} \end{array}$$

  for $a, b \in S$.

2.3.1. Upper and lower bounds, sup and inf. — Let S be a poset and let E be a subset of S.

- An *upper bound of E in S* is an element $b \in S$ such that if $y \in E$ then $y \leqslant b$.
- A *lower bound of E in S* is an element $l \in S$ such that if $y \in E$ then $l \leqslant y$.
- A *greatest lower bound of E in S* is an element $\inf(E) \in S$ such that
  (a) $\inf(E)$ is a lower bound of E in S, and
  (b) If $l \in S$ is a lower bound of E in S then $l \leqslant \inf(E)$.
- A *least upper bound of E in S* is an element $\sup(E) \in S$ such that

(a) $\sup(E)$ is a upper bound of E in S, and
(b) If $b \in S$ is a upper bound of E in S then $\sup(E) \leqslant b$.

- The set E is *bounded in S* if E has both an upper bound and a lower bound in S.

Proposition 2.3.1. — *Let S be a poset and let E be a subset of S. If* $\sup(E)$ *exists then* $\sup(E)$ *is unique.*

2.4. Fields and ordered fields

A *field* is a set $\mathbb{F}$ with functions

$$\begin{array}{ccc} \mathbb{F}\times\mathbb{F} & \longrightarrow & \mathbb{F} \\ (a,b) & \longmapsto & a+b \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathbb{F}\times\mathbb{F} & \longrightarrow & \mathbb{F} \\ (a,b) & \longmapsto & ab \end{array}$$

such that

(Fa) If $a,b,c \in \mathbb{F}$ then $(a+b)+c = a+(b+c)$,
(Fb) If $a,b \in \mathbb{F}$ then $a+b = b+a$,
(Fc) There exists $0 \in \mathbb{F}$ such that

$$\text{if } a \in \mathbb{F} \quad \text{then} \quad 0+a = a \text{ and } a+0 = a,$$

(Fd) If $a \in \mathbb{F}$ then there exists $-a \in \mathbb{F}$ such that $a+(-a) = 0$ and $(-a)+a = 0$,
(Fe) If $a,b,c \in \mathbb{F}$ then $(ab)c = a(bc)$,
(Ff) If $a,b,c \in \mathbb{F}$ then

$$(a+b)c = ac+bc \qquad \text{and} \qquad c(a+b) = ca+cb,$$

(Fg) There exists $1 \in \mathbb{F}$ such that

$$\text{if } a \in \mathbb{F} \quad \text{then} \quad 1\cdot a = a \text{ and } a\cdot 1 = a,$$

(Fh) If $a \in \mathbb{F}$ and $a \neq 0$ then there exists $a^{-1} \in \mathbb{F}$ such that $aa^{-1} = 1$ and $a^{-1}a = 1$,
(Fi) If $a,b \in \mathbb{F}$ then $ab = ba$.

Proposition 2.4.1. — *Let $\mathbb{F}$ be a field.*
(a) *If $a \in \mathbb{F}$ then $a \cdot 0 = 0$.*
(b) *If $a \in \mathbb{F}$ then $-(-a) = a$.*
(c) *If $a \in \mathbb{F}$ and $a \neq 0$ then $(a^{-1})^{-1} = a$.*
(d) *If $a \in \mathbb{F}$ then $a(-1) = -a$.*
(e) *If $a,b \in \mathbb{F}$ then $(-a)b = -ab$.*
(f) *If $a,b \in \mathbb{F}$ then $(-a)(-b) = ab$.*

2.4.1. Ordered fields. — An *ordered field* is a field $\mathbb{F}$ with a total order $\leqslant$ such that
(OFa) If $a,b,c \in \mathbb{F}$ and $a \leqslant b$ then $a+c \leqslant b+c$,
(OFb) If $a,b \in \mathbb{F}$ and $a \geqslant 0$ and $b \geqslant 0$ then $ab \geqslant 0$.

Proposition 2.4.2. — *Let $\mathbb{F}$ be an ordered field.*
(a) *If $a \in \mathbb{F}$ and $a > 0$ then $-a < 0$.*
(b) *If $a \in \mathbb{F}$ and $a \neq 0$ then $a^2 > 0$.*
(c) *$1 \geqslant 0$.*
(d) *If $a \in \mathbb{F}$ and $a > 0$ then $a^{-1} > 0$.*
(e) *If $a,b \in \mathbb{F}$ and $a \geqslant 0$ and $b \geqslant 0$ then $a+b \geqslant 0$.*
(f) *If $a,b \in \mathbb{F}$ and $0 < a < b$ then $b^{-1} < a^{-1}$.*

Proposition 2.4.3. — *Let $\mathbb{F}$ be an ordered field. Let $x, y \in \mathbb{F}$ with $x \geqslant 0$ and $y \geqslant 0$. Then*

$$x \leqslant y \qquad \text{if and only if} \qquad x^2 \leqslant y^2.$$

2.5. The binomial theorem and the exponential function

Let $k \in \mathbb{Z}_{\geqslant 0}$. Define k **factorial** by

$$0! = 1 \qquad \text{and} \qquad k! = k \cdot (k-1) \cdots 3 \cdot 2 \cdot 1 \text{ if } k \in \mathbb{Z}_{>0}.$$

Let $n, k \in \mathbb{Z}_{\geqslant 0}$ with $k \leqslant n$. Define

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Theorem 2.5.1. — *Let $n, k \in \mathbb{Z}_{\geqslant 0}$ with $k \leqslant n$.*
(a) Let S be a set with cardinality n. Then $\binom{n}{k}$ is the number of subsets of S with cardinality k.
(b) $\binom{n}{k}$ is the coefficient of $x^{n-k}y^k$ in $(x+y)^n$.
(c) If $k \in \{1, \ldots, n-1\}$ then

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \qquad \text{and} \qquad \binom{n}{0} = 1 \quad \text{and} \quad \binom{n}{n} = 1.$$

This theorem says that the table of numbers

$$\begin{array}{ccccccccccc}
 & & & & & \binom{0}{0} & & & & & \\
 & & & & \binom{1}{0} & & \binom{1}{1} & & & & \\
 & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & \\
 & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & \\
 & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & \\
\binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} \\
\ddots & & & & & \vdots & & & & & \ddots
\end{array}$$

are the numbers in **Pascal's triangle**

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
\ddots & & & & & \vdots & & & & & \ddots
\end{array}$$

and that

$$\begin{array}{rcc}
(x+y)^0 &=& 1, \\
(x+y)^1 &=& x+y, \\
(x+y)^2 &=& x^2+2xy+y^2, \\
(x+y)^3 &=& x^3+3x^2y+3xy^2+y^3, \\
(x+y)^4 &=& x^4+4x^3y+6x^2y^2+4xy^3+y^4, \\
(x+y)^5 &=& x^5+5x^4y+10x^3y^2+10x^2y^3+5xy^4+y^5, \\
\vdots & & \vdots
\end{array}$$

2.5.1. The exponential function. — The **exponential function** is the element e^x of $\mathbb{Q}[[x]]$ given by

$$e^x = \sum_{k\in\mathbb{Z}_{>0}} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots .$$

Theorem 2.5.2. — *As an element of* $\mathbb{Q}[[x,y]$ *(which has* $xy=yx$*),*

$$e^{x+y} = e^x e^y.$$

HW: Show that $e^0 = 1$.
HW: Show that $e^{-x} = \frac{1}{e^x}$.

The **logarithm** is

$$\log(1+x) = \sum_{k\in\mathbb{Z}_{>0}} (-1)^{k-1}\frac{x^k}{k} = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots .$$

Theorem 2.5.3. — *Let*

$$G = \{p(x) \in \mathbb{F}[[x]] \mid p(0) = 1\} \qquad \textit{and} \qquad \mathfrak{g} = \{p(x) \in \mathbb{Q}[[x]] \mid p(0) = 0\}$$

Then
(a) $\log(1+(e^x-1)) = e^{\log(1+x)} - 1 = x$.
(b) G is a commutative group under multiplication, $\mathfrak{g}$ is a commutative group under addition and

$$\begin{array}{ccc} G & \longrightarrow & \mathfrak{g} \\ p & \longmapsto & e^p - 1 \end{array} \quad \textit{is an isomorphism of groups.}$$

2.5.2. Notes and references. — The binomial theorem and 'Pascals triangle' are useful computational tools for multiplying out algebraic expressions. The exponential function "is the most important function in mathematics" [**Ru**, Prologue]. The theorems showing that the exponential function is a homomorphism and that the formal inverse to the exponential function is log are found in [**Bou**, Alg. Ch. IV §4 no. 10].

2.6. Notes and references

Almost everything in mathematics is built from sets and functions. Groups, rings, fields, vector spaces ... are all sets endowed with additional functions which have special properties. In the society of mathematics, sets and functions are the individuals and the fascination is the way that the individuals, each one different from the others, interact.

Functions are the morphisms in the category $\mathcal{S}$et of sets and products are products in the category $\mathcal{S}$et of all sets. The set of sets $\mathcal{S}$et may or may not make sense to you: there are good reasons – study Russell's paradox, the Zermelo-Frenkel axioms and small categories to learn more.

Fundamental definitions and properties of partially ordered sets are treated thoroughly in [Bou, Ens Ch. III]. The exposition of Stanley [St, Ch. 3] has an inspiring point of view and a wealth of information on the subject of posets. The definition of partially ordered set differs slightly depending on the author: Bourbaki replace axiom (a) in the definition by: If $x, y \in S$ and $x \leqslant y$ then $x \leqslant x$ and $y \leqslant y$. Bourbaki defines a preorder to be a partial order except without the axiom (b).

The set of subsets of a set S forms a partially ordered set under inclusion $\subseteq$. This is the favorite example of a partial order which is not a total order. The union $\cup$ and intersection $\cap$ make the set of subsets of S into a Boolean algebra. References for Boolean algebras are Birkhoff [Brk, Chapt X] and Stanley [St, §3.4]; in particular, the conditions for the finite Boolean algebra B_n are found in Stanley [St, p. 107-108].

The orders on the number systems $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are indispensible for ordinary daily measurements. Perhaps surprisingly, there is no partial order on $\mathbb{C}$ which makes $\mathbb{C}$ an ordered field.

The definitions of *left filtered* and *right filtered* are used in the theory of inverse and direct limits. The definitions and examples of upper and lower bounds, suprema and infima, maxima and minima, and largest and smallest element, are a natural way to introduce students to analyses and proofs of existence and uniqueness. Directed sets are the generalization of sequences used to define nets which, in turn, provide a general method for formaliing the notion of a limit (see notes of Arun Ram on filters and nets).

2.7. Proofs

2.7.1. An inverse function to f exists if and only if f is bijective.—

Theorem 2.7.1. — *Let $f\colon S \to T$ be a function. The inverse function to f exists if and only if f is bijective.*

Proof. —

$\Rightarrow$: Assume $f\colon S \to T$ has an inverse function $f^{-1}\colon T \to S$.

To show: (a) f is injective.

(b) f is surjective.

(a) Assume $s_1, s_2 \in S$ and $f(s_1) = f(s_2)$.

To show: $s_1 = s_2$.

$$s_1 = f^{-1}f(s_1)) = f^{-1}f(s_2)) = s_2.$$

So f is injective.

(b) Let $t \in T$.

To show: There exists $s \in S$ such that $f(s) = t$.

Let $s = f^{-1}(t)$.

Then

$$f(s) = f(f^{-1}(t)) = t.$$

So f is surjective.

So f is bijective.

$\Leftarrow$: Assume $f\colon S \to T$ is bijective.
To show: f has an inverse function.
We need to define a function $\varphi\colon T \to S$.
Let $t \in T$.
Since f is surjective there eists $s \in S$ such that $f(s) = t$.
Define $\varphi(t) = s$.
To show: (a) φ is well defined.
(b) φ is an inverse function to f.

(a) To show: (aa) If $t \in T$ then $\varphi(t) \in S$.
(ab) If $t_1, t_2 \in T$ and $t_1 = t_2$ then $\varphi(t_1) = \varphi(t_2)$.

(aa) This follows from the definition of φ.

(ab) Assume $t_1, t_2 \in T$ and $t_1 = t_2$.
Let $s_1, s_2 \in S$ such that $f(s_1) = t_1$ and $f(s_2) = t_2$.
Since $t_1 = t_2$ then $f(s_1) = f(s_2)$.
Since f is injective this implies that $s_1 = s_2$.
So $\varphi(t_1) = s_1 = s_2 = \varphi(t_2)$.

So φ is well defined.

(b) To show: (ba) If $s \in S$ then $\varphi(f(s)) = s$.
(bb) If $t \in T$ then $f(\varphi(t)) = t$.

(ba) This follows from the definition of φ.

(bb) Assume $t \in T$.
Let $s \in S$ be such that $f(s) = t$.
Then

$$f(\varphi(t)) = f(s) = t.$$

So $\varphi \circ f$ and $f \circ \varphi$ are the identity functions on S and T, respectively.

So φ is an inverse function to f.

□

2.7.2. An equivalence relation on S and a partition of S are the same data.—

Theorem 2.7.2. —

(a) *If S is a set and let $\sim$ be an equivalence relation on S then*

the set of equivalence classes of $\sim$ is a partition of S.

(b) *If S is a set and $\mathcal{P}$ is a partition of S then*

the relation defined by $s \sim t$ if s and t are in the same $P \in \mathcal{P}$

is an equivalence relation on S.

Proof. —

(a) To show: (aa) If $s \in S$ then s is in some equivalence class.
(ab) If $[s] \cap [t] \neq \emptyset$ then $[s] = [t]$.

(aa) Let $s \in S$.
Since $s \sim s$ then $s \in [s]$.

(ab) Assume $[s] \cap [t] \neq \emptyset$.
To show: $[s] = [t]$.
Since $[s] \cap [t] \neq \emptyset$ then there is an $r \in [s] \cap [t]$.

So $s \sim r$ and $r \sim t$.
By transitivity, $s \sim t$.
To show: (aba) $[s] \subseteq [t]$.
(abb) $[t] \subseteq [s]$.
(aba) Assume $u \in [s]$.
Then $u \sim s$.
We know $s \sim t$.
So, by transitivity, $u \sim t$.
Therefore $u \in [t]$.
So $[s] \subseteq [t]$.
(aba) Assume $v \in [t]$.
Then $v \sim t$.
We know $t \sim s$.
So, by transitivity, $v \sim s$.
Therefore $v \in [s]$.
So $[t] \subseteq [s]$.
So $[s] = [t]$.
So the equivalence classes partition S.

(b) To show: $\sim$ is an equivalence relation, i.e. that $\sim$ is reflexive, symmetric and transitive.
To show: (ba) If $s \in S$ then $s \sim s$.
(bb) If $s \sim t$ then $t \sim s$.
(bc) If $s \sim t$ and $t \sim u$ then $s \sim u$.
(ba) Since s and s are in the same S_α then $s \sim s$.
(bb) Assume $s \sim t$.
Then s and t are in the same S_α.
So $t \sim s$.
(bb) Assume $s \sim t$ and $t \sim u$.
Then s and t are in the same S_α and t and u are in the same S_α.
So $s \sim u$.
So $\sim$ is an equivalence relation.

□

2.7.3. Identities in a field. —

Proposition 2.7.3. — *Let $\mathbb{F}$ be a field.*
(a) *If $a \in \mathbb{F}$ then $a \cdot 0 = 0$.*
(b) *If $a \in \mathbb{F}$ then $-(-a) = a$.*
(c) *If $a \in \mathbb{F}$ and $a \neq 0$ then $(a^{-1})^{-1} = a$.*
(d) *If $a \in \mathbb{F}$ then $a(-1) = -a$.*
(e) *If $a, b \in \mathbb{F}$ then $(-a)b = -ab$.*
(f) *If $a, b \in \mathbb{F}$ then $(-a)(-b) = ab$.*

Proof. —

(a) Assume $a \in \mathbb{F}$.

$$\begin{aligned} a \cdot 0 &= a \cdot (0+0), \quad \text{by (Fc)}, \\ &= a \cdot 0 + a \cdot 0, \quad \text{by (Ff)}. \end{aligned}$$

Add $-a \cdot 0$ to each side and use (Fd) to get $0 = a \cdot 0$.

(b) Assume $a \in \mathbb{F}$.
By (Fd),

$$-(-a) + (-a) = 0 = a + (-a).$$

Add $-a$ to each side and use (Fd) to get $-(-a) = a$.

(c) Assume $a \in \mathbb{F}$ and $a \neq 0$.
By (Fh),

$$(a^{-1})^{-1} \cdot a^{-1} = 1 = a \cdot a^{-1}.$$

Multiply each side by a and use (Fh) and (Fg) to get $(a^{-1})^{-1} = a$.

(d) Assume $a \in \mathbb{F}$.
By (Ff),

$$a(-1) + a \cdot 1 = a(-1+1) = a \cdot 0 = 0,$$

where the last equality follows from part (a).
So, by (Fg), $a(-1) + a = 0$.
Add $-a$ to each side and use (Fd) and (Fc) to get $a(-1) = -a$.

(e) Assume $a, b \in \mathbb{F}$.

$$\begin{aligned} (-a)b + ab &= (-a+a)b, \quad \text{by (Ff)}, \\ &= 0 \cdot b, \quad \text{by (Fd)}, \\ &= 0, \quad \text{by part (a)}. \end{aligned}$$

Add $-ab$ to each side and use (Fd) and (Fc) to get $(-a)b = -ab$.

(f) Assume $a, b \in \mathbb{F}$.

$$\begin{aligned} (-a)(-b) &= -(a(-b)), \quad \text{by (e)}, \\ &= -(-ab), \quad \text{by (e)}, \\ &= ab, \quad \text{by part (b)}. \end{aligned}$$

□

2.7.4. Identities in an ordered field. —

Proposition 2.7.4. — *Let $\mathbb{F}$ be an ordered field.*
(a) *If $a \in \mathbb{F}$ and $a > 0$ then $-a < 0$.*
(b) *If $a \in \mathbb{F}$ and $a \neq 0$ then $a^2 > 0$.*
(c) *$1 \geqslant 0$.*
(d) *If $a \in \mathbb{F}$ and $a > 0$ then $a^{-1} > 0$.*
(e) *If $a, b \in \mathbb{F}$ and $a \geqslant 0$ and $b \geqslant 0$ then $a + b \geqslant 0$.*
(f) *If $a, b \in \mathbb{F}$ and $0 < a < b$ then $b^{-1} < a^{-1}$.*

Proof. —

(a) Assume $a \in \mathbb{F}$ and $a > 0$.
Then $a + (-a) > 0 + (-a)$, by (OFb).

So $0 > -a$, by (Fd) and (Fc).

(b) Assume $a \in \mathbb{F}$ and $a \neq 0$.

Case 1: $a > 0$.

Then $a \cdot a > a \cdot 0$, by (OFb).

So $a^2 > 0$, by part (a).

Case 2: $a < 0$.

Then $-a > 0$, by part (a).

Then $(-a)^2 > 0$, by Case 1.

So $a^2 > 0$, by Proposition 13.4.3 (f).

(c) To show: $1 \geqslant 0$.

$1 = 1^2 \geqslant 0$, by part (b).

(d) Assume $a \in \mathbb{F}$ and $a > 0$.

By part (b), $a^{-2} = (a^{-1})^2 > 0$.

So $a(a^{-1})^2 > a \cdot 0$, by (OFb).

So $a^{-1} > 0$, by (Fh) and Proposition 13.4.3 (a).

(e) Assume $a, b \in \mathbb{F}$ and $a \geqslant 0$ and $b \geqslant 0$.

$$\begin{aligned} a + b &\geqslant 0 + b, \quad \text{by (OFa)},\\ &\geqslant 0 + 0, \quad \text{by (OFa)},\\ &= 0, \quad \text{by (Fc)}. \end{aligned}$$

(f) Assume $a, b \in \mathbb{F}$ and $0 < a < b$.

So $a > 0$ and $b > 0$.

Then, by part (d), $a^{-1} > 0$ and $b^{-1} > 0$.

Thus, by (OFb), $a^{-1}b^{-1} > 0$.

Since $a < b$, then $b - a > 0$, by (OFa).

So, by (OFb), $a^{-1}b^{-1}(b-a) > 0$.

So, by (Fh), $a^{-1} - b^{-1} > 0$.

So, by (OFa), $a^{-1} > y^{-1}$.

□

2.7.5. The binomial theorem. —

Theorem 2.7.5. — *Let $n, k \in \mathbb{Z}_{\geqslant 0}$ with $k \in \{0, 1, \ldots, n\}$. Assume $xy = yx$.*
(a) If $k \in \{1, \ldots, n-1\}$ then

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \qquad \textit{and} \qquad \binom{n}{0} = 1 \quad \textit{and} \quad \binom{n}{n} = 1.$$

(b) $\binom{n}{k}$ is the coefficient of $x^{n-k}y^k$ in $(x+y)^n$.
(c) Let S be a set with cardinality n.
Then $\binom{n}{k}$ is the number of subsets of S with cardinality k.
(d) $e^{(x+y)} = e^x e^y$.

Proof. — (a) $\binom{n}{0} = \frac{n!}{0!(n-0)!} = \frac{n!}{1\cdot n!} = 1$ and $\binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{n!}{n!0!} = \frac{n!}{n!\cdot 1} = 1$.
If $k \in \{1, \ldots, n-1\}$ then

$$\begin{aligned}\binom{n-1}{k-1} + \binom{n-1}{k-1} &= \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!} \\ &= \frac{(n-1)!}{(k-1)!(n-1-k)!}\Big(\frac{1}{n-k} + \frac{1}{k}\Big) \\ &= \frac{(n-1)!}{(k-1)!(n-1-k)!}\,\frac{n}{k(n-k)} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.\end{aligned}$$

(b) The base cases are $(x+y)^0 = 1 = \binom{0}{0}x^0y^0$ and $(x+y)^1 = x+y = \binom{1}{0}x^1y^0 + \binom{1}{1}x^1y^0$. Then, by induction,

$$\begin{aligned}(x+y)^n &= (x+y)^{n-1}(x+y) \\ &= \Big(\binom{n-1}{0}x^{n-1}y^0 + \binom{n-1}{1}x^{n-2}y^1 + \cdots + \binom{n-1}{n-2}x^1y^{n-2} + \binom{n-1}{n-1}x^0y^{n-1}\Big)(x+y) \\ &= \binom{n-1}{0}x^ny^0 + \binom{n-1}{1}x^{n-1}y^1 + \cdots + \binom{n-1}{n-2}x^2y^{n-2} + \binom{n-1}{n-1}x^1y^{n-1} \\ &\qquad + \binom{n-1}{0}x^{n-1}y^1 \qquad + \cdots + \binom{n-1}{n-2}x^1y^{n-1} + \binom{n-1}{n-1}x^0y^n \\ &= \binom{n}{0}x^ny^0 \quad + \binom{n}{1}x^{n-1}y^1 \qquad + \cdots + \binom{n}{n-1}x^1y^{n-1} + \binom{n}{n}x^0y^n,\end{aligned}$$

where the last equality follows from part (a).

(c) Since

$$\begin{aligned}(x+y)^n = \underbrace{(x+y)\cdots(x+y)}_{n \text{ factors}} &= \sum_{k=0}^{n} \sum_{\substack{J\subseteq\{1,\ldots,n\} \\ \mathrm{Card}(J)=k}} \Big(\prod_{\substack{i\in\{1,\ldots,n\} \\ i\notin J}} x\Big)\Big(\prod_{\substack{j\in\{1,\ldots,n\} \\ j\in J}} y\Big) \\ &= \sum_{k=0}^{n} \mathrm{Card}(\{J \subseteq \{1,\ldots,n\} \mid \mathrm{Card}(J) = k\})\, x^{n-k}y^k,\end{aligned}$$

the coefficient of $x^{n-k}y^k$ is the number of ways of choosing k factors (each of which comtributes a y to $x^{n-k}y^k$) from the n factors in $(x+y)\cdots(x+y) = (x+y)^n$.

(d)

$$
\begin{aligned}
e^{(x+y)} &= 1 + (x+y) + \frac{1}{2!}(x+y)^2 + \frac{1}{3!}(x+y)^3 + \cdots \\
&= \begin{array}{c}
1 \\
+(x+y) \\
+\tfrac{1}{2!}(x^2 + 2xy + y^2) \\
+\tfrac{1}{3!}(x^3 + 3x^2y + 3xy^2 + y^3) \\
+\tfrac{1}{4!}(x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4) \\
+\tfrac{1}{5!}(x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5) \\
\vdots
\end{array} \\
&= \begin{array}{c}
1 \\
+x + y \\
+\tfrac{1}{2!}x^2 + xy + \tfrac{1}{2!}y^2 \\
+\tfrac{1}{3!}x^3 + \tfrac{1}{2!}x^2y + x\tfrac{1}{2!}y^2 + \tfrac{1}{3!}y^3 \\
+\tfrac{1}{4!}x^4 + \tfrac{1}{3!}x^3y + \tfrac{1}{2!}x^2\tfrac{1}{2!}y^2 + x\tfrac{1}{3!}y^3 + \tfrac{1}{4!}y^4 \\
+\tfrac{1}{5!}x^5 + \tfrac{1}{4!}x^4y + \tfrac{1}{3!}x^3\tfrac{1}{2!}y^2 + \tfrac{1}{2!}x^2\tfrac{1}{3!}y^3 + x\tfrac{1}{4!}y^4 + \tfrac{1}{5!}y^5 \\
\vdots
\end{array} \\
&= e^x + e^x y + e^x \frac{1}{2!}y^2 + e^x \frac{1}{3!}y^3 + \cdots \quad = e^x e^y,
\end{aligned}
$$

where the next to last equality follows by adding up the diagonals. □

2.8. Exercises