Set Theory

Marcel Schütz

2021

Abstract

This is a formalization of some ZF-like set theory. It introduces the common operations on sets like unions, intersections, complements, powersets, symmetric differences and Cartesian products and presents detailled proofs of their algebraic properties. Moreover, basic notions concerning functions like images, preimages and invertibility are provided, again with detailed proofs of their computation laws, up to the definition of equipollency.

It can either be regarded as an independent collection of contents from basic undergraduate mathematics or serve as the basis for more sophisticated formalizations.

Contents

Part I
Sets

1 Sets

[readtex `vocabulary.ftl.tex`]

[readtex `macros.ftl.tex`]

We base our formalization on the notions of classes, sets and objects which are hardcoded into $\mathbb{N}$aproche.

Let x, y, z denote sets.

Sets are regarded as classes which are also objects, the latter being entities that are in some sense small enough to be contained in classes.

Axiom 1.1. x is a class.

Axiom 1.2. x is an objects.

Axiom 1.3. Let u be an element of x. Then u is an object.

1.1 Subsets

Let us continue with the notion of *subsets*, i.e. sets which are included in some other set.

Definition 1.4. A subset of x is a set y such that every element of y is an element of x.

Let $y \subseteq x$ stand for y is a subset of x. Let $y \subset x$ stand for $y \subseteq x$. Let a superset of x stand for a set y such that $x \subseteq y$. Let $y \supseteq x$ stand for y is a superset of x. Let $y \supset x$ stand for $y \supseteq x$. Let x includes y stand for $y \subseteq x$. Let y is included in x stand for x includes y.

Definition 1.5. A proper subset of x is a subset of x that is not equal to x.

Let $y \subsetneq x$ stand for x is a proper subset of x. Let a proper superset of x stand for a set y such that $x \subsetneq y$. Let $y \supsetneq x$ stand for y is a proper superset of x.

Proposition 1.6. $x \subseteq x$.

Proposition 1.7. If $x \subseteq y$ and $y \subseteq z$ then $x \subseteq z$.

1.2 Set extensionality

Since the only distinguishing feature of a set should be its elements, let us add the following *extensionality axiom* to our theory.

Axiom 1.8 (Set extensionality). If $x \subseteq y$ and $y \subseteq x$ then $x = y$.

1.3 Separation

Our next axiom ensures that the universe of sets is closed under taking subcollections. This means that any subcollection of a given set is itself a set.

Axiom 1.9 (Separation). Let C be a collection and x be a set. Assume that every element of C is contained in x. Then C is a set.

1.4 Set existence

Up to now our theory does not admit the existence of a single set. This is changed by the following axiom.

Axiom 1.10 (Set existence). There exists a set.

1.5 The empty set

The last to axioms allow us now to show that there exists a unique set that does not contain any element – the *empty* set.

Definition 1.11. x is empty iff x has no elements.

Let x is nonempty stand for x is not empty.

Lemma 1.12. There exists an empty set.

Proof. Define $C = \{ u \mid \text{contradiction} \}$. Take a set x (by Set existence). Then every element of C is contained in x. Hence C is a set (by Separation). C has no element. Hence the thesis. $\square$

Lemma 1.13. If x and y are empty then $x = y$.

Proof. Assume that x and y are empty. Then every element of x is an element of y and every element of y is an element of x. Hence $x \subseteq y$ and $y \subseteq x$. Thus $x = y$. $\square$

Definition 1.14. $\emptyset$ is the empty set.

Let $\{\}$ stand for $\emptyset$. Let the empty set stand for $\emptyset$.

Proposition 1.15. $\emptyset$ is a subset of every set.

Proof. Let x be a set. Then every element of $\emptyset$ is an element of x. Indeed $\emptyset$ has no element. Hence $\emptyset \subseteq x$. $\square$

1.6 Pairing

Let us now consider an axiom which allows us to collect two given objects into a set which contains exactly these two ones.

Axiom 1.16 (Pairing). Let u, v be objects. There exists a set z such that $z = \{ w \mid w = u \text{ or } w = v \}$.

Definition 1.17. Let u, v be elements. $\{u, v\}$ is the set z such that $z = \{ w \mid w = u \text{ or } w = v \}$.

Let the unordered pair of u and v stand for $\{u, v\}$.

Lemma 1.18. Let u be an element. There exists a set z such that $z = \{ w \mid w = u \}$.

Proof. Take $z = \{u, u\}$. Then $z = \{ w \mid w = u \}$. $\square$

Definition 1.19. Let u be an element. $\{u\}$ is the set z such that $z = \{ w \mid w = u \}$.

Let the singleton set of u stand for $\{u\}$.

Definition 1.20. A singleton set is a set x such that $x = \{u\}$ for some element u.

1.7 Set-systems

Sets whose elements are all sets as well are called *set- systems* or *systems of sets*.

Definition 1.21. A system of sets is a set X such that every element of X is a set.

Let X, Y, Z denote systems of sets.
Let a set of X stand for an element of X.

Definition 1.22. A system of nonempty sets is a system of sets X such that every set of X is nonempty.

Proposition 1.23. $\{x\}$ is a system of sets.

Proposition 1.24. $\{x, y\}$ is a system of sets.

Definition 1.25. A system of subsets of x is a set X such that every set of X is a subset of x.

Proposition 1.26. Every system of subsets of x is a system of sets.

1.8 Intersections

Considering a set-system X we can extract all objects which are contained in *every* member of X into a new set, called the *intersection* over X.

Lemma 1.27. Let x be a nonempty system of sets. Then there exists a set z such that $z = \{ u \mid u \text{ is contained in every member of } x \}$.

Proof. Take an element y of x. Then y is a set. (1) Define $z = \{ u \mid u \text{ is contained in every element of } x \}$. Every element of z is contained in y. Hence z is a set. Therefore the thesis (by 1). ☐

Definition 1.28. Let x be a nonempty system of sets. $\bigcap x$ is the set z such that $z = \{ u \mid u \text{ is contained in every member of } x \}$.

Let the intersection over x stand for $\bigcap x$.

The notion of the intersection over a set-system can be used to provide an operation which maps two sets to the set of all elements they have in common.

Lemma 1.29. Let x, y be sets. Then there exists a set z such that $z = \{ u \mid u \in x \text{ and } u \in y \}$.

Proof. Take $z = \bigcap\{x, y\}$. Then

$$z = \{ u \mid u \text{ is contained in every element of } \{x, y\} \} .$$

Hence $z = \{ u \mid u \in x \text{ and } u \in y \}$. ☐

Definition 1.30. $x \cap y$ is the set z such that $z = \{ u \mid u \in x \text{ and } u \in y \}$.

Let the intersection of x and y stand for $x \cap y$.

Proposition 1.31. $\bigcap\{x, y\} = x \cap y$.

Proof. Let us show that $\bigcap\{x, y\} \subseteq x \cap y$. Let $u \in \bigcap\{x, y\}$. Then u is an element of every element of $\{x, y\}$. Hence $u \in x$ and $u \in y$. Thus $u \in x \cap y$. End.

Let us show that $x \cap y \subseteq \bigcap\{x, y\}$. Let $u \in x \cap y$. Then $u \in x$ and $u \in y$. Hence u is an element of every element of $\{x, y\}$. Thus $u \in \bigcap\{x, y\}$. End. ☐

Corollary 1.32. $\bigcap\{x\} = x$.

Proof. $\bigcap\{x\} = \bigcap\{x, x\} = x \cap x = x$. ☐

Proposition 1.33. Let x be a nonempty system of sets. Then $y \subseteq \bigcap x$ iff y is a subset of every element of x.

Proof. Case $y \subseteq \bigcap x$. Let z be an element of x. Let $u \in y$. Then $u \in \bigcap x$. Hence $u \in z$. End.

Case y is a subset of every element of x. Let $u \in y$. Then $u \in z$ for all sets z such that $z \in x$. Hence $u \in \bigcap x$. End. $\square$

An important notion is that of *disjoint* sets, i.e. sets wich do not have any elements in common.

Definition 1.34. x and y are disjoint iff $x \cap y = \emptyset$.

Obviously this yields a symmetric relation on the universe of sets.

Proposition 1.35. If x and y are disjoint then y and x are disjoint.

Proof. Assume that x and y are disjoint. Then $x \cap y$ is empty. Hence there is no element u such that $u \in x$ and $u \in y$. Thus $y \cap x$ is empty. Therefore y and x are disjoint. $\square$

1.9 Unions

Analogous to the definition of the intersection over a set-system we now want to consider for a given set-system X the collection of all elements which lie in *some* member of X. To ensure that this collection is a set we need an additional axiom.

Axiom 1.36 (Union). Let x be a system of sets. Then there exists a set z such that $z = \{ u \mid u \text{ is contained in some element of } x \}$.

Definition 1.37. Let x be a system of sets. $\bigcup x$ is the set z such that $z = \{ u \mid u \text{ is contained in some element of } x \}$.

Let the union over x stand for $\bigcup x$.

Lemma 1.38. Let x, y be sets. Then there exists a set z such that $z = \{ u \mid u \in x \text{ or } u \in y \}$.

Proof. Take $z = \bigcup\{x, y\}$. Then

$$z = \{ u \mid u \text{ is contained in some element of } \{x, y\} \} .$$

Hence $z = \{ u \mid u \in x \text{ or } u \in y \}$. $\square$

Definition 1.39. $x \cup y$ is the set z such that $z = \{ w \mid w \in x \text{ or } w \in y \}$.

Let the union of x and y stand for $x \cup y$.

Proposition 1.40. $\bigcup\{x, y\} = x \cup y$.

Proof. Let us show that $\bigcup\{x, y\} \subseteq x \cup y$. Let $u \in \bigcup\{x, y\}$. Then u is an element of some element of $\{x, y\}$. Hence $u \in x$ or $u \in y$. Thus $u \in x \cup y$. End.

Let us show that $x \cup y \subseteq \bigcup\{x, y\}$. Let $u \in x \cup y$. Then $u \in x$ or $u \in y$. Hence u is an element of some element of $\{x, y\}$. Thus $u \in \bigcup\{x, y\}$. End. $\square$

Corollary 1.41. $\bigcup\{x\} = x$.

Proof. $\bigcup\{x\} = \bigcup\{x, x\} = x \cup x = x$. □

Proposition 1.42. Let x be a system of sets. Then $\bigcup x \subseteq y$ iff every element of x is a subset of y.

Proof. Case $\bigcup x \subseteq y$. Let z be an element of x. Let $u \in z$. Then u is an element of some element of x. Hence $u \in \bigcup x$. Thus $u \in y$. End.

Case every element of x is a subset of y. Let $u \in \bigcup x$. Take a set z such that $z \in x$ and $u \in z$. Then z is a subset of y. Hence $u \in y$. End. □

Proposition 1.43. $\bigcup \emptyset = \emptyset$.

Proof. $\emptyset$ has no elements. Hence there is no $x \in \emptyset$ that has an element. Thus $\bigcup \emptyset$ is empty. Therefore $\bigcup \emptyset = \emptyset$. □

1.10 Partitions

Another important notion is that of a *partition* of a set x. i.e. a set which splits x into pairwise disjoint subsets.

Definition 1.44. A partition of x is a system of sets P such that every element of P is a subset of x and every element of x is contained in some member of P and all distinct sets A, B of P are pairwise disjoint.

Proposition 1.45. Let P be a partition of x. Then $x = \bigcup P$.

Proof. Let us show that $x \subseteq \bigcup P$. Let $u \in x$. Take a set A of P such that $u \in A$. Then we have $u \in \bigcup P$. End.

Let us show that $\bigcup P \subseteq x$. Let $u \in \bigcup P$. Then we can take a set A of P such that $u \in A$. A is a subset of x. Hence $u \in x$. End. □

1.11 Complements

Let us define another operation on sets: The *(relative) complement*.

Lemma 1.46. Let x, y be sets. There exists a set z such that $z = \{ w \mid w \in x \text{ and } w \notin y \}$.

Proof. Define $z = \{ w \mid w \in x \text{ and } w \notin y \}$. Then every element of z is contained in x. Hence z is a set (by Separation). □

Definition 1.47. $x \setminus y$ is the set such that $x \setminus y = \{ w \mid w \in x \text{ and } w \notin y \}$.

Let the complement of y in x stand for $x \setminus y$.

1.12 Computation laws

Now that we are provided with the most common operations on sets let us have a look on their algebraic properties.

Commutativity of union and intersection:

Proposition 1.48.

$$x \cup y = y \cup x.$$

Proof. Let us show that $x \cup y \subseteq y \cup x$. Let $u \in x \cup y$. Then $u \in x$ or $u \in y$. Hence $u \in y$ or $u \in x$. Thus $u \in y \cup x$. End.

Let us show that $y \cup x \subseteq x \cup y$. Let $u \in y \cup x$. Then $u \in y$ or $u \in x$. Hence $u \in x$ or $u \in y$. Thus $u \in x \cup y$. End. ☐

Proposition 1.49.

$$x \cap y = y \cap x.$$

Proof. Let us show that $x \cap y \subseteq y \cap x$. Let $u \in x \cap y$. Then $u \in x$ and $u \in y$. Hence $u \in y$ and $u \in x$. Thus $u \in y \cap x$. End.

Let us show that $y \cap x \subseteq x \cap y$. Let $u \in y \cap x$. Then $u \in y$ and $u \in x$. Hence $u \in x$ and $u \in y$. Thus $u \in x \cap y$. End. ☐

Associativity of union and intersection:

Proposition 1.50.

$$((x \cup y) \cup z) = x \cup (y \cup z).$$

Proof. Let us show that $((x \cup y) \cup z) \subseteq x \cup (y \cup z)$. Let $u \in (x \cup y) \cup z$. Then $u \in x \cup y$ or $u \in z$. Hence $u \in x$ or $u \in y$ or $u \in z$. Thus $u \in x$ or $u \in (y \cup z)$. Therefore $u \in x \cup (y \cup z)$. End.

Let us show that $x \cup (y \cup z) \subseteq (x \cup y) \cup z$. Let $u \in x \cup (y \cup z)$. Then $u \in x$ or $u \in y \cup z$. Hence $u \in x$ or $u \in y$ or $u \in z$. Thus $u \in x \cup y$ or $u \in z$. Therefore $u \in (x \cup y) \cup z$. End. □

Proposition 1.51.

$$((x \cap y) \cap z) = x \cap (y \cap z).$$

Proof. Let us show that $((x \cap y) \cap z) \subseteq x \cap (y \cap z)$. Let $u \in (x \cap y) \cap z$. Then $u \in x \cap y$ and $u \in z$. Hence $u \in x$ and $u \in y$ and $u \in z$. Thus $u \in x$ and $u \in (y \cap z)$. Therefore$u \in x \cap (y \cap z)$. End.

Let us show that $x \cap (y \cap z) \subseteq (x \cap y) \cap z$. Let $u \in x \cap (y \cap z)$. Then $u \in x$ and $u \in y \cap z$. Hence $u \in x$ and $u \in y$ and $u \in z$. Thus $u \in x \cap y$ and $u \in z$. Therefore$u \in (x \cap y) \cap z$. End. □

Distributivity of union and intersection:

Proposition 1.52.

$$x \cap (y \cup z) = (x \cap y) \cup (x \cap z).$$

Proof. Let us show that $x \cap (y \cup z) \subseteq (x \cap y) \cup (x \cap z)$. Let $u \in x \cap (y \cup z)$. Then $u \in x$ and $u \in y \cup z$. Hence $u \in x$ and ($u \in y$ or $u \in z$). Thus ($u \in x$ and $u \in y$) or ($u \in x$ and $u \in z$). Therefore $u \in x \cap y$ or $u \in x \cap z$. Hence $u \in (x \cap y) \cup (x \cap z)$. End.

Let us show that $((x \cap y) \cup (x \cap z)) \subseteq x \cap (y \cup z)$. Let $u \in (x \cap y) \cup (x \cap z)$. Then $u \in x \cap y$ or $u \in x \cap z$. Hence ($u \in x$ and $u \in y$) or ($u \in x$ and $u \in z$). Thus $u \in x$ and ($u \in y$ or $u \in z$). Therefore $u \in x$ and $u \in y \cup z$. Hence$u \in x \cap (y \cup z)$. End. □

Proposition 1.53.

$$x \cup (y \cap z) = (x \cup y) \cap (x \cup z).$$

Proof. Let us show that $x \cup (y \cap z) \subseteq (x \cup y) \cap (x \cup z)$. Let $u \in x \cup (y \cap z)$. Then $u \in x$ or $u \in y \cap z$. Hence $u \in x$ or ($u \in y$ and $u \in z$). Thus ($u \in x$ or $u \in y$) and ($u \in$ x or $u \in z$). Therefore $u \in x \cup y$ and $u \in x \cup z$. Hence $u \in (x \cup y) \cap (x \cup z)$. End.

Let us show that $((x \cup y) \cap (x \cup z)) \subseteq x \cup (y \cap z)$. Let $u \in (x \cup y) \cap (x \cup z)$. Then $u \in x \cup y$ and $u \in x \cup z$. Hence ($u \in x$ or $u \in y$) and ($u \in x$ or $u \in z$). Thus $u \in x$ or ($u \in y$ and $u \in z$). Therefore $u \in x$ or $u \in y \cap z$. Hence $u \in x \cup (y \cap z)$. End. □

Idempocy laws for union and intersection:

Proposition 1.54.

$$x \cup x = x.$$

Proof. $x \cup x = \{ u \mid u \in x \text{ or } u \in x \}$. Hence $x \cup x = \{ u \mid u \in x \}$. Thus $x \cup x = x$. □

Proposition 1.55.

$$x \cap x = x.$$

Proof. $x \cap x = \{ u \mid u \in x \text{ and } u \in x \}$. Hence $x \cap x = \{ u \mid u \in x \}$. Thus $x \cap x = x$. □

Distributivity of complement wrt. union and intersection:

Proposition 1.56.

$$x \setminus (y \cap z) = (x \setminus y) \cup (x \setminus z).$$

Proof. Let us show that $x \setminus (y \cap z) \subseteq (x \setminus y) \cup (x \setminus z)$. Let $u \in x \setminus (y \cap z)$. Then $u \in x$ and $u \notin y \cap z$. Hence it is wrong that ($u \in y$ and $u \in z$). Thus $u \notin y$ or $u \notin z$. Therefore $u \in x$ and ($u \notin y$ or $u \notin z$). Then ($u \in x$ and $u \notin y$) or ($u \in x$ and $u \notin z$). Hence $u \in x \setminus y$ or $u \in x \setminus z$. Thus $u \in (x \setminus y) \cup (x \setminus z)$. End.

Let us show that $((x \setminus y) \cup (x \setminus z)) \subseteq x \setminus (y \cap z)$. Let $u \in (x \setminus y) \cup (x \setminus z)$. Then $u \in x \setminus y$ or $u \in x \setminus z$. Hence ($u \in x$ and $u \notin y$) or ($u \in x$ and $u \notin z$). Thus $u \in x$ and ($u \notin y$ or $u \notin z$). Therefore $u \in x$ and not ($u \in y$ and $u \in z$). Then $u \in x$ and not $u \in y \cap z$. Hence $u \in x \setminus (y \cap z)$. End. □

Proposition 1.57.

$$x \setminus (y \cup z) = (x \setminus y) \cap (x \setminus z).$$

Proof. Let us show that $x \setminus (y \cup z) \subseteq (x \setminus y) \cap (x \setminus z)$. Let $u \in x \setminus (y \cup z)$. Then $u \in x$ and $u \notin y \cup z$. Hence it is wrong that ($u \in y$ or $u \in z$). Thus $u \notin y$ and $u \notin z$. Therefore $u \in x$ and ($u \notin y$ and $u \notin z$). Then ($u \in x$ and $u \notin y$) and ($u \in x$ and $u \notin z$). Hence $u \in x \setminus y$ and $u \in x \setminus z$. Thus $u \in (x \setminus y) \cap (x \setminus z)$. End.

Let us show that $((x \setminus y) \cap (x \setminus z)) \subseteq x \setminus (y \cup z)$. Let $u \in (x \setminus y) \cap (x \setminus z)$. Then $u \in x \setminus y$ and $u \in x \setminus z$. Hence ($u \in x$ and $u \notin y$) and ($u \in x$ and

$u \notin z$). Thus $u \in x$ and ($u \notin y$ and $u \notin z$). Therefore $u \in x$ and not ($u \in y$ or $u \in z$). Then $u \in x$ and not $u \in y \cup z$. Hence $u \in x \setminus (y \cup z)$. End. □

Subset laws:

Proposition 1.58.

$$x \subseteq x \cup y.$$

Proof. Let $u \in x$. Then $u \in x$ or $u \in y$. Hence $u \in x \cup y$. □

Proposition 1.59.

$$x \cap y \subseteq x.$$

Proof. Let $u \in x \cap y$. Then $u \in x$ and $u \in y$. Hence $u \in x$. □

Proposition 1.60.

$$x \subseteq y \iff x \cup y = y.$$

Proof. Case $x \subseteq y$.

Let us show that $x \cup y \subseteq y$. Let $u \in x \cup y$. Then $u \in x$ or $u \in y$. If $u \in x$ then $u \in y$. Hence $u \in y$. End.

Let us show that $y \subseteq x \cup y$. Let $u \in y$. Then $u \in x$ or $u \in y$. Hence $u \in x \cup y$. End. End.

Case $x \cup y = y$. Let $u \in x$. Then $u \in x$ or $u \in y$. Hence $u \in x \cup y = y$. End. □

Proposition 1.61.

$$x \subseteq y \iff x \cap y = x.$$

Proof. Case $x \subseteq y$.

Let us show that $x \cap y \subseteq x$. Let $u \in x \cap y$. Then $u \in x$ and $u \in y$. Hence $u \in x$. End.

Let us show that $x \subseteq x \cap y$. Let $u \in x$. Then $u \in y$. Hence $u \in x$ and $u \in y$. Thus $u \in x \cap y$. End. End.

Case $x \cap y = x$. Let $u \in x$. Then $u \in x \cap y$. Hence $u \in x$ and $u \in y$. Thus $u \in y$. End. □

Complement laws:

Proposition 1.62.

$$x \setminus x = \emptyset.$$

Proof. $x \setminus x$ has no elements. Indeed $x \setminus x = \{ u \mid u \in x \text{ and } u \notin x \}$. Hence the thesis. □

Proposition 1.63.
$$x \setminus \emptyset = x.$$

Proof. $x \setminus \emptyset = \{ u \mid u \in x \text{ and } u \notin \emptyset \}$. No element is an element of $\emptyset$. Hence $x \setminus \emptyset = \{ u \mid u \in x \}$. Then we have the thesis. □

Proposition 1.64.
$$x \setminus (x \setminus y) = x \cap y.$$

Proof. Let us show that $x \setminus (x \setminus y) \subseteq x \cap y$. Let $u \in x \setminus (x \setminus y)$. Then $u \in x$ and $u \notin x \setminus y$. Hence $u \notin x$ or $u \in y$. Thus $u \in y$. Therefore $u \in x \cap y$. End.

Let us show that $x \cap y \subseteq x \setminus (x \setminus y)$. Let $u \in x \cap y$. Then $u \in x$ and $u \in y$. Hence $u \notin x$ or $u \in y$. Thus $u \notin x \setminus y$. Therefore $u \in x \setminus (x \setminus y)$. End. □

Proposition 1.65.
$$y \subseteq x \iff x \setminus (x \setminus y) = y.$$

Proof. Case $y \subseteq x$. Obvious.

Case $x \setminus (x \setminus y) = y$. Then every element of y is an element of $x \setminus (x \setminus y)$. Thus every element of y is an element of x. Then we have the thesis. End. □

Proposition 1.66.
$$x \cap (y \setminus z) = (x \cap y) \setminus (x \cap z).$$

Proof. Let us show that $x \cap (y \setminus z) \subseteq (x \cap y) \setminus (x \cap z)$. Let $u \in x \cap (y \setminus z)$. Then $u \in x$ and $u \in y \setminus z$. Hence $u \in x$ and $u \in y$. Thus $u \in x \cap y$ and $u \notin z$. Therefore $u \notin x \cap z$. Then we have $u \in (x \cap y) \setminus (x \cap z)$. End.

Let us show that $((x \cap y) \setminus (x \cap z)) \subseteq x \cap (y \setminus z)$. Let $u \in (x \cap y) \setminus (x \cap z)$. Then $u \in x$ and $u \in y$. $u \notin x \cap z$. Hence $u \notin z$. Thus $u \in y \setminus z$. Therefore $u \in x \cap (y \setminus z)$. End. □

2 The powerset

[readtex `set-theory/sections/01_sets/01_sets.ftl.tex`]

Let u, v, w denote objects. Let x, y, z denote sets.

In this paragraph we consider collections of subsets of a given set. To ensure that these are sets themselves, we need another axiom.

Axiom 2.1 (Powerset). There exists a set z such that $z = \{ y \mid y \subseteq x \}$.

Definition 2.2. $\mathcal{P}(x)$ is the set z such that $z = \{ y \mid y \subseteq x \}$.

Let the powerset of x stand for $\mathcal{P}(x)$.

Proposition 2.3. $\emptyset$ and x are elements of $\mathcal{P}(x)$.

Proof. We have $\emptyset, x \subseteq x$. Hence the thesis. □

Corollary 2.4. $\mathcal{P}(x)$ is nonempty.

Proposition 2.5. $\mathcal{P}(x)$ is a system of subsets of x.

Proposition 2.6. $\bigcup \mathcal{P}(x) = x$.

Proof. Every element of $\mathcal{P}(x)$ is a subset of x. Hence $\bigcup \mathcal{P}(x) \subseteq x$.

We have $x \in \mathcal{P}(x)$. Hence every element of x is an element of some element of $\mathcal{P}(x)$. Thus every element of x belongs to $\bigcup \mathcal{P}(x)$. Therefore $x \subseteq \bigcup \mathcal{P}(x)$.

Then we have the thesis. □

Proposition 2.7. $\bigcap \mathcal{P}(x) = \emptyset$.

Proof. We have $\emptyset \in \mathcal{P}(x)$. Hence every element of $\bigcap \mathcal{P}(x)$ is an element of $\emptyset$. Thus $\bigcap \mathcal{P}(x)$ is empty. Therefore $\bigcap \mathcal{P}(x) = \emptyset$. □

3 The axiom of regularity

[readtex `set-theory/sections/01_sets/01_sets.ftl.tex`]

Let u, v, w denote objects. Let x, y, z denote sets.

The *axiom of regularity* (or *axiom of foundation*) states that every non-empty set has a $\in$-minimal element.

Axiom 3.1 (Regularity). Every nonempty set x that contains some set contains some set y such that x and y are disjoint.

As a consequence we get that no set can contain itself. Moreover, this allows us to show that there exists no universal set, i.e. that "the set of all sets" does not exist.

Proposition 3.2. No set x is an element of x.

Proof. Assume the contrary. Take a set x such that $x \in x$. We can take an element y of $\{x\}$ such that $\{x\}$ and y are disjoint (by Regularity). Indeed $\{x\}$ contains some set. Then $y = x$. Hence $\{x\}$ and x are disjoint. Contradiction. Indeed $x \in \{x\}$ and $x \in x$. □

Corollary 3.3. There is no set that contains every set.

Proof. Assume the contrary. Take a set V that contains every set. Then V is an element of V. Contradiction. □

Proposition 3.4. There exist no sets x, y such that $x \in y$ and $y \in x$.

Proof. Assume the contrary. Take sets x, y such that $x \in y$ and $y \in x$. Consider an element z of $\{x, y\}$ such that $\{x, y\}$ and z are disjoint (by Regularity). Indeed $\{x, y\}$ contains some set. We have $z = x$ or $z = y$.

Case $z = x$. Then x and $\{x, y\}$ are disjoint. Hence $y \notin x$. Contradiction. End.

Case $z = y$. Then y and $\{x, y\}$ are disjoint. Hence $x \notin y$. Contradiction. End. □

4 The symmetric difference

[readtex `set-theory/sections/01_sets/01_sets.ftl.tex`]

Let u, v, w denote objects. Let x, y, z denote sets.

It is time to indroduce a new operation on sets: The *symmetric difference*.

4.1 Definition

The symmetric difference of two sets is the set of all objects wich are contained in *exactly one* of these sets.

Definition 4.1. $x \triangle y = (x \cup y) \setminus (x \cap y)$.

Let the symmetric difference of x and y stand for $x \triangle y$.

Lemma 4.2. $x \triangle y$ is a set.

Proof. x and y are sets. Hence $x \cup y$ and $x \cap y$ are sets. Thus $(x \cup y) \setminus (x \cap y)$ is a set. Therefore $x \triangle y$ is a set. □

Alternatively, we could have defined the symmetric difference as follows:

Proposition 4.3. $x \triangle y = (x \setminus y) \cup (y \setminus x)$.

Proof. Let us show that $x \triangle y \subseteq (x \setminus y) \cup (y \setminus x)$. Let $u \in x \triangle y$. Then $u \in x \cup y$ and $u \notin x \cap y$. Hence ($u \in x$ or $u \in y$) and not ($u \in x$ and $u \in y$). Thus ($u \in x$ or $u \in y$) and ($u \notin x$ or $u \notin y$). Therefore if $u \in x$ then $u \notin y$. If $u \in y$ then $u \notin x$. Then we have ($u \in x$ and $u \notin y$) or ($u \in y$ and $u \notin x$). Hence $u \in x \setminus y$ or $u \in y \setminus x$. Thus $u \in (x \setminus y) \cup (y \setminus x)$. End.

Let us show that $((x \setminus y) \cup (y \setminus x)) \subseteq x \triangle y$. Let $u \in (x \setminus y) \cup (y \setminus x)$. Then $(u \in x$ and $u \notin y)$ or $(u \in y$ and $u \notin x)$. If $u \in x$ and $u \notin y$ then $u \in x \cup y$ and $u \notin x \cap y$. If $u \in y$ and $u \notin x$ then $u \in x \cup y$ and $u \notin x \cap y$. Hence $u \in x \cup y$ and $u \notin x \cap y$. Thus $u \in (x \cup y) \setminus (x \cap y) = x \triangle y$. End. □

4.2 Computation laws

As we did with our previously introduced set operations let us prove some of the most important algebraic properties of the symmetric difference.

Commutativity:

Proposition 4.4.

$$x \triangle y = y \triangle x.$$

Proof. $x \triangle y = (x \cup y) \setminus (x \cap y) = (y \cup x) \setminus (y \cap x) = y \triangle x$. □

Associativity:

Proposition 4.5.

$$((x \triangle y) \triangle z) = x \triangle (y \triangle z).$$

Proof. Take $A = (((x \setminus y) \cup (y \setminus x)) \setminus z) \cup (z \setminus ((x \setminus y) \cup (y \setminus x)))$.

Take $B = (x \setminus ((y \setminus z) \cup (z \setminus y))) \cup (((y \setminus z) \cup (z \setminus y)) \setminus x)$.

We have $x \triangle y = (x \setminus y) \cup (y \setminus x)$ and $y \triangle z = (y \setminus z) \cup (z \setminus y)$. Hence $(x \triangle y) \triangle z = A$ and $x \triangle (y \triangle z) = B$.

Let us show that (A) $A \subseteq B$. Let $u \in A$.

(A 1) Case $u \in ((x \setminus y) \cup (y \setminus x)) \setminus z$. Then $u \notin z$.

(A 1a) Case $u \in x \setminus y$. Then $u \notin y \setminus z$ and $u \notin z \setminus y$. $u \in x$. Hence $u \in x \setminus ((y \setminus z) \cup (z \setminus y))$. Thus $u \in B$. End.

(A 1b) Case $u \in y \setminus x$. Then $u \in y \setminus z$. Hence $u \in (y \setminus z) \cup (z \setminus y)$. $u \notin x$. Thus $u \in ((y \setminus z) \cup (z \setminus y)) \setminus x$. Therefore $u \in B$. End. End.

(A 2) Case $u \in z \setminus ((x \setminus y) \cup (y \setminus x))$. Then $u \in z$. $u \notin x \setminus y$ and $u \notin y \setminus x$. Hence not $(u \in x \setminus y$ or $u \in y \setminus x)$. Thus not $((u \in x$ and $u \notin y)$ or $(u \in y$ and $u \notin x))$. Therefore $(u \notin x$ or $u \in y)$ and $(u \notin y$ or $u \in x)$.

(A 2a) Case $u \in x$. Then $u \in y$. Hence $u \notin (y \setminus z) \cup (z \setminus y)$. Thus $u \in x \setminus ((y \setminus z) \cup (z \setminus y))$. Therefore $u \in B$. End.

(A 2b) Case $u \notin x$. Then $u \notin y$. Hence $u \in z \setminus y$. Thus $u \in (y \setminus z) \cup (z \setminus y)$. Therefore $u \in ((y \setminus z) \cup (z \setminus y)) \setminus x$. Then we have $u \in B$. End. End. End.

Let us show that (B) $B \subseteq A$. Let $u \in B$.

(B 1) Case $u \in x \setminus ((y \setminus z) \cup (z \setminus y))$. Then $u \in x$. $u \notin y \setminus z$ and $u \notin z \setminus y$. Hence not ($u \in y \setminus z$ or $u \in z \setminus y$). Thus not (($u \in y$ and $u \notin z$) or ($u \in z$ and $u \notin y$)). Therefore ($u \notin y$ or $u \in z$) and ($u \notin z$ or $u \in y$).

(B 1a) Case $u \in y$. Then $u \in z$. $u \notin x \setminus y$ and $u \notin y \setminus x$. Hence $u \notin (x \setminus y) \cup (y \setminus x)$. Thus $u \in z \setminus ((x \setminus y) \cup (y \setminus x))$. Therefore $u \in A$. End.

(B 1b) Case $u \notin y$. Then $u \notin z$. $u \in x \setminus y$. Hence $u \in (x \setminus y) \cup (y \setminus x)$. Thus $u \in ((x \setminus y) \cup (y \setminus x)) \setminus z$. Therefore $u \in A$. End. End.

(B 2) Case $u \in ((y \setminus z) \cup (z \setminus y)) \setminus x$. Then $u \notin x$.

(B 2a) Case $u \in y \setminus z$. Then $u \in y \setminus x$. Hence $u \in (x \setminus y) \cup (y \setminus x)$. Thus $u \in ((x \setminus y) \cup (y \setminus x)) \setminus z$. Therefore $u \in A$. End.

(B 2b) Case $u \in z \setminus y$. Then $u \in z$. $u \notin x \setminus y$ and $u \notin y \setminus x$. Hence $u \notin (x \setminus y) \cup (y \setminus x)$. Thus $u \in z \setminus ((x \setminus y) \cup (y \setminus x))$. Therefore $u \in A$. End. End. End. □

Distributivity of intersection and symmetric difference:

Proposition 4.6.

$$x \cap (y \triangle z) = (x \cap y) \triangle (x \cap z).$$

Proof. $x \cap (y \triangle z) = x \cap ((y \setminus z) \cup (z \setminus y)) = (x \cap (y \setminus z)) \cup (x \cap (z \setminus y))$.

$x \cap (y \setminus z) = (x \cap y) \setminus (x \cap z)$. $x \cap (z \setminus y) = (x \cap z) \setminus (x \cap y)$.

Hence $x \cap (y \triangle z) = ((x \cap y) \setminus (x \cap z)) \cup ((x \cap z) \setminus (x \cap y)) = (x \cap y) \triangle (x \cap z)$. □

Miscellaneous rules:

Proposition 4.7.

$$x \subseteq y \iff x \triangle y = y \setminus x.$$

Proof. Case $x \subseteq y$. Then $x \cup y = y$ and $x \cap y = x$. Hence the thesis. End.

Case $x \triangle y = y \setminus x$. Let $u \in x$. Then $u \notin y \setminus x$. Hence $u \notin x \triangle y$. Thus $u \notin x \cup y$ or $u \in x \cap y$. Indeed $x \triangle y = (x \cup y) \setminus (x \cap y)$. If $u \notin x \cup y$ then we have a contradiction. Therefore $u \in x \cap y$. Then we have the thesis. End. □

Proposition 4.8.

$$x \triangle y = x \triangle z \iff y = z.$$

Proof. Case $x \triangle y = x \triangle z$.

Let us show that $y \subseteq z$. Let $u \in y$.

Case $u \in x$. Then $u \notin x \triangle y$. Hence $u \notin x \triangle z$. Therefore $u \in x \cap z$. Indeed $x \triangle z = (x \cup z) \setminus (x \cap z)$. Hence $u \in z$. End.

Case $u \notin x$. Then $u \in x \triangle y$. Indeed $u \in x \cup y$ and $u \notin x \cap y$. Hence $u \in x \triangle z$. Thus $u \in x \cup z$ and $u \notin x \cap z$. Therefore $u \in x$ or $u \in z$. Then we have the thesis. End. End.

Let us show that $z \subseteq y$. Let $u \in z$.

Case $u \in x$. Then $u \notin x \triangle z$. Hence $u \notin x \triangle y$. Therefore $u \in x \cap y$. Indeed $u \notin x \cup y$ or $u \in x \cap y$. Hence $u \in y$. End.

Case $u \notin x$. Then $u \in x \triangle z$. Indeed $u \in x \cup z$ and $u \notin x \cap z$. Hence $u \in x \triangle y$. Thus $u \in x \cup y$ and $u \notin x \cap y$. Therefore $u \in x$ or $u \in y$. Then we have the thesis. End. End. End. ☐

Proposition 4.9.

$$x \triangle x = \emptyset.$$

Proof. $x \triangle x = (x \cup x) \setminus (x \cap x) = x \setminus x = \emptyset$. ☐

Proposition 4.10.

$$x \triangle \emptyset = x.$$

Proof. $x \triangle \emptyset = (x \cup \emptyset) \setminus (x \cap \emptyset) = x \setminus \emptyset = x$. ☐

Proposition 4.11.

$$x = y \iff x \triangle y = \emptyset.$$

Proof. Case $x = y$. Then $x \triangle y = (x \cup x) \setminus (x \cap x) = x \setminus x = \emptyset$. Hence the thesis. End.

Case $x \triangle y = \emptyset$. Then $(x \cup y) \setminus (x \cap y)$ is empty. Hence every element of $x \cup y$ is an element of $x \cap y$. Thus for all elements u if $u \in x$ or $u \in y$ then $u \in x$ and $u \in y$. Therefore every element of x is an element of y. Every element of y is an element of x. Then we have the thesis. End. ☐

5 Ordered pairs

[readtex `set-theory/sections/01_sets/01_sets.ftl.tex`]

Let u, v, w, u', v', w' denote objects. Let x, y, z, x', y', z' denote sets.

In this paragraph we introduce the *ordered pair* of two objects, following the definition proposed by Kuratowski.

Note that Naproche has ordered pairs already built in. Thus we have to formulate the definition of them as an axiom.

Axiom 5.1. $(u, v) = \{\{u\}, \{u, v\}\}$.

Proposition 5.2. Let u, v be objects. Then (u, v) is an object.

Proof. $\{u\}$ and $\{u, v\}$ are objects. Hence $\{\{u\}, \{u, v\}\}$ is an object. We have $(u, v) = \{\{u\}, \{u, v\}\}$. Thus (u, v) is an object. □

The central property of ordered pairs is that two of them agree if they agree on each component.

Proposition 5.3. If $(u, v) = (u', v')$ then $u = u'$ and $v = v'$.

Proof. Assume $(u, v) = (u', v')$. (1) Then $\{\{u\}, \{u, v\}\} = \{\{u'\}, \{u', v'\}\}$. Hence ($\{u\} = \{u'\}$ or $\{u\} = \{u', v'\}$) and ($\{u, v\} = \{u'\}$ or $\{u, v\} = \{u', v'\}$). Thus ($\{u\} = \{u'\}$ and ($\{u, v\} = \{u'\}$ or $\{u, v\} = \{u', v'\}$)) or ($\{u\} = \{u', v'\}$ and ($\{u, v\} = \{u'\}$ or $\{u, v\} = \{u', v'\}$)).

Case $\{u\} = \{u'\}$ and ($\{u, v\} = \{u'\}$ or $\{u, v\} = \{u', v'\}$). We have $\{u\} = \{u'\}$. Hence $u = u'$.

Case $\{u, v\} = \{u'\}$. Then $u = u' = v$. Hence $\{\{u\}, \{u, u\}\} = \{\{u\}, \{u, v'\}\}$ (by 1). Thus $\{\{u\}\} = \{\{u\}, \{u, v'\}\}$. Therefore $\{u\} = \{u, v'\}$. Consequently $v' = u = v$. End.

Case $\{u, v\} = \{u', v'\}$. Then $\{u, v\} = \{u, v'\}$. Hence $v = v'$. End. End.

Case $\{u\} = \{u', v'\}$ and ($\{u, v\} = \{u'\}$ or $\{u, v\} = \{u', v'\}$). We have $\{u\} = \{u', v'\}$. Hence $u = u'$.

Case $\{u, v\} = \{u'\}$. Then $u = v = u'$. Hence $v = v'$. End.

Case $\{u, v\} = \{u', v'\}$. Then $\{u, v\} = \{u, v'\}$. Hence $v = v'$. End. End. □

Definition 5.4. A pair is an object x such that $x = (u, v)$ for some objects u, v.

Let an ordered pair stand for a pair.

Definition 5.5. Let x be a pair. The first component of x is the object u such that $x = (u, v)$ for some object v.

Let the first entry of x stand for the first component of x.

Definition 5.6. Let x be a pair. The second component of x is the object v such that $x = (u, v)$ for some object u.

Let the second entry of x stand for the second component of x.

Lemma 5.7. Let x be a pair. Let u be the first component of x and v be the second component of x. Then $x = (u, v)$.

Lemma 5.8. Let x, y be pairs. Assume that the first component of x agrees with the first component of y and the second component of x agrees with the second component of y. Then $x = y$.

6 Cartesian products

[readtex `set-theory/sections/01_sets/02_powerset.ftl.tex`]

[readtex `set-theory/sections/01_sets/05_ordered-pairs.ftl.tex`]

Let u, v, w, u', v', w' denote objects. Let x, y, z, x', y', z' denote sets.

Let us now consider collections of ordered pairs. We can show that for any given sets x, y the collection of all pairs whose first component lies in x and whose second component lies in y is a set. This set is called the *Cartesian product* of x and y.

Lemma 6.1. There exists a set z such that

$$z = \{ (u, v) \mid u \in x \text{ and } v \in y \} .$$

Proof. (1) Define $z = \{ (u, v) \mid u \in x \text{ and } v \in y \}$. Take $z' = \mathcal{P}(\mathcal{P}(x \cup y))$. Then z' is a set.

Let us show that every element of z is contained in z'. Let $w \in z$. Take elements u, v such that $w = (u, v)$. Then $u \in x$ and $v \in y$. Hence $\{u\}$ and $\{u, v\}$ are subsets of $x \cup y$. Thus $\{u\}$ and $\{u, v\}$ are elements of $\mathcal{P}(x \cup y)$. Therefore $w = \{\{u\}, \{u, v\}\} \subseteq \mathcal{P}(x \cup y)$. Consequently $w \in \mathcal{P}(\mathcal{P}(x \cup y)) = z'$. End.

Hence z is a set (by Separation). Therefore the thesis (by 1). □

Definition 6.2. $x \times y$ is the set z such that $z = \{ (u, v) \mid u \in x \text{ and } v \in y \}$.

Let the Cartesian product of x and y stand for $x \times y$.

Proposition 6.3. $(u, v) \in x \times y$ iff $u \in x$ and $v \in y$.

Proof. Case $(u, v) \in x \times y$. We can take $u' \in x$ and $v' \in y$ such that $(u, v) = (u', v')$. Then $u = u'$ and $v = v'$. Hence $u \in x$ and $v \in y$. End.

Case $u \in x$ and $v \in y$. u and v are elements. Hence (u, v) is an element. Therefore $(u, v) \in x \times y$. Indeed $x \times y = \{ (u', v') \mid u' \in x \text{ and } v' \in y \}$. End. □

Proposition 6.4. $x \times y$ is empty iff x is empty or y is empty.

Proof. Case $x \times y$ is empty. Assume that x and y are nonempty. Thus we can take an element u of x and an element v of y. Then (u, v) is an element of $x \times y$. Contradiction. End.

Case x is empty or y is empty. Assume that $x \times y$ is nonempty. Then we can take an element z of $x \times y$. Then $z = (u, v)$ for some $u \in x$ and some $v \in y$. Hence x and y are nonempty. Contradiction. End. □

Proposition 6.5. $\{u\} \times \{v\} = \{(u, v)\}$.

Proof. Let us show that $\{u\} \times \{v\} \subseteq \{(u, v)\}$. Let $w \in \{u\} \times \{v\}$. Take $a \in \{u\}$ and $b \in \{v\}$ such that $w = (a, b)$. We have $a = u$ and $b = v$. Hence $w = (u, v)$. Thus $w \in \{(u, v)\}$. End.

Let us show that $\{(u, v)\} \subseteq \{u\} \times \{v\}$. Let $w \in \{(u, v)\}$. Then $w = (u, v)$. We have $u \in \{u\}$ and $v \in \{v\}$. Hence $w \in \{u\} \times \{v\}$. End. $\square$

6.1 Computation laws

As always let us have a look at the algebraic properties of our new operation.

Subset laws:

Proposition 6.6.

$$x \subseteq y \implies x \times z \subseteq y \times z.$$

Proof. Assume $x \subseteq y$. Let $w \in x \times z$. Take $u \in x$ and $v \in z$ such that $w = (u, v)$. Then $u \in y$. Hence $(u, v) \in y \times z$. $\square$

Proposition 6.7. Assume that x and x' are nonempty.

$$(x \times x') \subseteq (y \times y') \iff (x \subseteq y \text{ and } x' \subseteq y').$$

Proof. Case $(x \times x') \subseteq (y \times y')$. Let us show that for all $u \in x$ and all $v \in x'$ we have $u \in y$ and $v \in y'$. Let $u \in x$ and $v \in x'$. Then $(u, v) \in x \times x'$. Hence $(u, v) \in y \times y'$. Thus $u \in y$ and $v \in y'$. End. End.

Case $x \subseteq y$ and $x' \subseteq y'$. Let $w \in x \times x'$. Take $u \in x$ and $v \in x'$ such that $w = (u, v)$. Then $u \in y$ and $v \in y'$. Hence $(u, v) \in y \times y'$. End. $\square$

Distributivity of product and union:

Proposition 6.8.

$$((x \cup y) \times z) = (x \times z) \cup (y \times z).$$

Proof. Let us show that $((x \cup y) \times z) \subseteq (x \times z) \cup (y \times z)$. Let $w \in (x \cup y) \times z$. Take $u \in x \cup y$ and $v \in z$ such that $w = (u, v)$. Then $u \in x$ or $u \in y$. If $u \in x$ then $w \in x \times z$ and if $u \in y$ then $w \in y \times z$. Hence $w \in x \times z$ or $w \in y \times z$. Thus $w \in (x \times z) \cup (y \times z)$. End.

Let us show that $((x \times z) \cup (y \times z)) \subseteq (x \cup y) \times z$. Let $w \in (x \times z) \cup (y \times z)$. Then $w \in x \times z$ or $w \in y \times z$. Take elements u, v such that $w = (u, v)$. Then ($u \in x$ or $u \in y$) and $v \in z$. Hence $u \in x \cup y$. Thus $w \in (x \cup y) \times z$. End. $\square$

Proposition 6.9.

$$x \times (y \cup z) = (x \times y) \cup (x \times z).$$

Proof. Let us show that $x \times (y \cup z) \subseteq (x \times y) \cup (x \times z)$. Let $w \in x \times (y \cup z)$. Take $u \in x$ and $v \in y \cup z$ such that $w = (u, v)$. Then $v \in y$ or $v \in z$. Hence $w \in x \times y$ or $w \in x \times z$. Indeed if $v \in y$ then $w \in x \times y$ and if $v \in z$ then $w \in x \times z$. Thus $w \in (x \times y) \cup (x \times z)$. End.

Let us show that $((x \times y) \cup (x \times z)) \subseteq x \times (y \cup z)$. Let $w \in (x \times y) \cup (x \times z)$. Then $w \in x \times y$ or $w \in x \times z$. Take elements u, v such that $w = (u, v)$. Then $u \in x$ and ($v \in y$ or $v \in z$). Hence $w \in x \times (y \cup z)$. End. □

Distributivity of product and intersection:

Proposition 6.10.

$$((x \cap y) \times z) = (x \times z) \cap (y \times z).$$

Proof. Let us show that $((x \cap y) \times z) \subseteq (x \times z) \cap (y \times z)$. Let $w \in (x \cap y) \times z$. Take $u \in x \cap y$ and $v \in z$ such that $w = (u, v)$. Then $u \in x$ and $u \in y$. Hence $w \in x \times z$ and $w \in y \times z$. Thus $w \in (x \times z) \cap (y \times z)$. End.

Let us show that $((x \times z) \cap (y \times z)) \subseteq (x \cap y) \times z$. Let $w \in (x \times z) \cap (y \times z)$. Then $w \in x \times z$ and $w \in y \times z$. Take elements u, v such that $w = (u, v)$. Then ($u \in x$ and $u \in y$) and $v \in z$. Hence $u \in x \cap y$. Thus $w \in (x \cap y) \times z$. End. □

Proposition 6.11.

$$x \times (y \cap z) = (x \times y) \cap (x \times z).$$

Proof. Let us show that $x \times (y \cap z) \subseteq (x \times y) \cap (x \times z)$. Let $w \in x \times (y \cap z)$. Take $u \in x$ and $v \in y \cap z$ such that $w = (u, v)$. Then $v \in y$ and $v \in z$. Hence $w \in x \times y$ and $w \in x \times z$. Thus $w \in (x \times y) \cap (x \times z)$. End.

Let us show that $((x \times y) \cap (x \times z)) \subseteq x \times (y \cap z)$. Let $w \in (x \times y) \cap (x \times z)$. Then $w \in x \times y$ and $w \in x \times z$. Take elements u, v such that $w = (u, v)$. Then $u \in x$ and ($v \in y$ and $v \in z$). Hence $w \in x \times (y \cap z)$. End. □

Distributivity of product and complement:

Proposition 6.12.

$$((x \setminus y) \times z) = (x \times z) \setminus (y \times z).$$

Proof. Let us show that $((x \setminus y) \times z) \subseteq (x \times z) \setminus (y \times z)$. Let $w \in (x \setminus y) \times z$.

Take $u \in x \setminus y$ and $v \in z$ such that $w = (u, v)$. Then $u \in x$ and $u \notin y$. Hence $w \in x \times z$ and $w \notin y \times z$. Thus $w \in (x \times z) \setminus (y \times z)$. End.

Let us show that $((x \times z) \setminus (y \times z)) \subseteq (x \setminus y) \times z$. Let $w \in (x \times z) \setminus (y \times z)$. Then $w \in x \times z$ and $w \notin y \times z$. Take $u \in x$ and $v \in z$ such that $w = (u, v)$. Then $u \notin y$. Indeed if $u \in y$ then $w \in y \times z$. Hence $u \in x \setminus y$. Thus $w \in (x \setminus y) \times z$. End. □

Proposition 6.13.

$$x \times (y \setminus z) = (x \times y) \setminus (x \times z).$$

Proof. Let us show that $x \times (y \setminus z) \subseteq (x \times y) \setminus (x \times z)$. Let $w \in x \times (y \setminus z)$. Take $u \in x$ and $v \in y \setminus z$ such that $w = (u, v)$. Then $v \in y$ and $v \notin z$. Hence $w \in x \times y$ and $w \notin x \times z$. Thus $w \in (x \times y) \setminus (x \times z)$. End.

Let us show that $((x \times y) \setminus (x \times z)) \subseteq x \times (y \setminus z)$. Let $w \in (x \times y) \setminus (x \times z)$. Then $w \in x \times y$ and $w \notin x \times z$. Take elements u, v such that $w = (u, v)$. Then $u \in x$ and ($v \in y$ and $v \notin z$). Hence $w \in x \times (y \setminus z)$. End. □

Equality law:

Proposition 6.14. Assume that x and x' are nonempty or y and y' are nonempty. Then

$$(x \times x') = (y \times y') \iff (x = y \text{ and } x' = y').$$

Proof. Case $x \times x' = y \times y'$. Then x and x' are nonempty iff y and y' are nonempty.

Let us show that for all $u \in x$ and all $v \in x'$ we have $u \in y$ and $v \in y'$. Let $u \in x$ and $v \in x'$. Then $(u, v) \in x \times x'$. Hence we can take $w \in y \times y'$ such that $w = (u, v)$. Thus $u \in y$ and $v \in y'$. End.

Therefore $x \subseteq y$ and $x' \subseteq y'$. Indeed x and x' are nonempty.

Let us show that for all $u \in y$ and all $v \in y'$ we have $u \in x$ and $v \in x'$. Let $u \in y$ and $v \in y'$. Then $(u, v) \in y \times y'$. Hence we can take $w \in x \times x'$ such that $w = (u, v)$. Thus $(u, v) \in x \times x'$. End.

Therefore $y \subseteq x$ and $y' \subseteq x'$. Indeed y and y' are nonempty. End.

Case $x = y$ and $x' = y'$. Trivial. □

Intersection of products:

Proposition 6.15.

$$((x \times y) \cap (x' \times y')) = (x \cap x') \times (y \cap y').$$

Proof. Let us show that $((x \times y) \cap (x' \times y')) \subseteq (x \cap x') \times (y \cap y')$. Let $w \in (x \times y) \cap (x' \times y')$. Then $w \in x \times y$ and $w \in x' \times y'$. Take elements u, v such that $w = (u, v)$. Then $u \in x, x'$ and $v \in y, y'$. Hence $u \in x \cap x'$ and $v \in y \cap y'$. Thus $w \in (x \cap x') \times (y \cap y')$. End.

Let us show that $(x \cap x') \times (y \cap y') \subseteq (x \times y) \cap (x' \times y')$. Let $w \in (x \cap x') \times (y \cap y')$. Take elements u, v such that $w = (u, v)$. Then $u \in x \cap x'$ and $v \in y \cap y'$ (by 6.3). Hence $u \in x, x'$ and $v \in y, y'$. Thus $w \in x \times y$ and $w \in x' \times y'$. Therefore $w \in (x \times y) \cap (x' \times y')$. End. □

Union of products:

Proposition 6.16.

$$((x \times y) \cup (x' \times y')) \subseteq (x \cup x') \times (y \cup y').$$

Proof. Let $w \in (x \times y) \cup (x' \times y')$. Then $w \in x \times y$ or $w \in x' \times y'$. Take elements u, v such that $w = (u, v)$. Then ($u \in x$ or $u \in x'$) and ($v \in y$ or $v \in y'$). Hence $u \in x \cup x'$ and $v \in y \cup y'$. Thus $w \in (x \cup x') \times (y \cup y')$. □

Complement of products:

Proposition 6.17.

$$((x \times y) \setminus (x' \times y')) = (x \times (y \setminus y')) \cup ((x \setminus x') \times y).$$

Proof. Let us show that $((x \times y) \setminus (x' \times y')) \subseteq (x \times (y \setminus y')) \cup ((x \setminus x') \times y)$. Let $w \in (x \times y) \setminus (x' \times y')$. Then $w \in x \times y$ and $w \notin x' \times y'$. Take $u \in x$ and $v \in y$ such that $w = (u, v)$. Then it is wrong that $u \in x'$ and $v \in y'$. Hence $u \notin x'$ or $v \notin y'$. Thus $u \in x \setminus x'$ or $v \in y \setminus y'$. Therefore $w \in x \times (y \setminus y')$ or $w \in (x \setminus x') \times y$. Hence we have $w \in (x \times (y \setminus y')) \cup ((x \setminus x') \times y)$. End.

Let us show that $(x \times (y \setminus y')) \cup ((x \setminus x') \times y) \subseteq (x \times y) \setminus (x' \times y')$. Let $w \in (x \times (y \setminus y')) \cup ((x \setminus x') \times y)$. Then $w \in (x \times (y \setminus y'))$ or $w \in ((x \setminus x') \times y)$. Take elements u, v such that $w = (u, v)$. Then ($u \in x$ and $v \in y \setminus y'$) or ($u \in x \setminus x'$ and $v \in y$) (by 6.3).

Case $u \in x$ and $v \in y \setminus y'$. Then $u \in x$ and $v \in y$. Hence $w \in x \times y$. We have $v \notin y'$. Thus $w \notin x' \times y'$. Therefore $w \in (x \times y) \setminus (x' \times y')$. End.

Case $u \in x \setminus x'$ and $v \in y$. Then $u \in x$ and $v \in y$. Hence $w \in x \times y$. We

have $u \notin x'$. Thus $w \notin x' \times y'$. Therefore $w \in (x \times y) \setminus (x' \times y')$. End.
End. $\square$

Part II
Functions

7 Functions

[readtex `set-theory/sections/01_sets/01_sets.ftl.tex`]

Let u, v, w denote objects. Let x, y, z denote sets. Let f, g, h denote functions.

In this section we introduce the notion of *functions* as some kind of "small" maps, i.e. maps whose domains are sets and whose values are objects.

7.1 Function axioms

Definition 7.1. Let f be a map. A value of f is an object v such that $v = f(u)$ for some $u \in \mathrm{dom}(f)$.

Definition 7.2. A fixed point of f is an element u of the domain of f such that $f(u) = u$.

As with sets we give an *extentionality axiom* for functions, which asserts that two functions are identical if their domains and values agree.

Axiom 7.3 (Function extensionality). Let f, g be functions. If $\mathrm{dom}(f) = \mathrm{dom}(g)$ and $f(u) = g(u)$ for all $u \in \mathrm{dom}(f)$ then $f = g$.

Since functions are already built-in notions of Naproche we cannot introduce them via a definition such as the following:

Definition. A function is a map f such that $\mathrm{dom}(f)$ is a set and every value of f is an object.

Instead we have to describe them axiomatically.

Axiom 7.4. Let f be a map. Assume that $\mathrm{dom}(f)$ is a set. Assume that every value of f is an object. Then f is a function.

Axiom 7.5. Let f be a function. Then f is a map.

Axiom 7.6. Let f be a function. Then $\mathrm{dom}(f)$ is a set.

Axiom 7.7. Let f be a function. Let x be an element of $\mathrm{dom}(f)$. Then $f(x)$ is an object.

The next axiom we introduce does not just fulfil definitional purposes. Instead it ensures that the image of any set under an arbitrary *mapping* is also a set. It plays an important role in the construction of certain infinite sets.

Axiom 7.8 (Replacement). Let f be a map and x be a set. There exists a set y such that $y = \{ f(u) \mid u \in \mathrm{dom}(f) \text{ and } u \in x \}$.

Corollary 7.9. Let f be a function. There exists a set y such that $y = \{ f(u) \mid u \in \mathrm{dom}(f) \}$.

Proof. Take $x = \mathrm{dom}(f)$. Then x is a set. Hence we can take a set y such that $y = \{ f(u) \mid u \in \mathrm{dom}(f) \}$ (by Replacement). Indeed f is a map. $\square$

7.2 The range

Using the replacement axiom we can easily define the *range* of a function as the set of all its values.

Definition 7.10. Let f be a function. $\mathrm{range}(f)$ is the set y such that $y = \{ f(u) \mid u \in \mathrm{dom}(f) \}$.

Let the range of f stand for $\mathrm{range}(f)$.

Proposition 7.11. v is a value of f iff $v \in \mathrm{range}(f)$.

Proof. Case v is a value of f. Take $u \in \mathrm{dom}(f)$ such that $v = f(u)$. v is an element. Hence $v \in \mathrm{range}(f)$. End.

Case $v \in \mathrm{range}(f)$. Then $v = f(u)$ for some $u \in \mathrm{dom}(f)$. Hence v is a value of f. End. $\square$

7.3 Functions between sets

In the following we mostly want to consider functions *between* two sets x and y, i.e. functions whose domain is x and which maps all elements of x into y.

Definition 7.12. A function of x is a function f such that $\mathrm{dom}(f) = x$.

Definition 7.13. A function to y is a function f such that $f(u) \in y$ for all $u \in \mathrm{dom}(f)$.

Let a function from x to y stand for a function f of x such that f is a function to y. Let $f : x \to y$ stand for f is a function from x to y.

Proposition 7.14. Let f be a function from x to y. Then $\mathrm{range}(f) \subseteq y$.

Proof. Let $v \in \mathrm{range}(f)$. Take $u \in x$ such that $v = f(u)$. Then $v \in y$. $\square$

Definition 7.15. A function on x is a function from x to x.

There are three important types of functions: Functions which are *injective*, i.e. one-to-one correspondences between their domain and range, functions which are *surjrective*, i.e. whose values match all elements of a given set, and functions which are *bijective*, i.e. both *injective* and *surjective*.

Definition 7.16. A function onto y is a function f such that $y = \mathrm{range}(f)$.

Let f surjects onto y stand for $y = \mathrm{range}(f)$.

Definition 7.17. A function from x onto y is a function f of x such that f is a function onto y.

Let $f : x \twoheadrightarrow y$ stand for f is a function from x onto y.

Proposition 7.18. f is a function onto $\mathrm{range}(f)$.

Proposition 7.19. Let f be a function onto y. Then f is a function to y.

Proof. Let $u \in \mathrm{dom}(f)$. Then $f(u) \in \mathrm{range}(f)$. Hence $f(u) \in y$. □

Definition 7.20. f is one to one iff for all $u, v \in \mathrm{dom}(f)$ if $f(u) = f(v)$ then $u = v$.

Definition 7.21. A function into y is an one to one function to y.

Definition 7.22. A function from x into y is a function f of x such that f is a function into y.

Let $f : x \hookrightarrow y$ stand for f is a function from x into y.

Definition 7.23. A bijection between x and y is a one to one function f from x onto y.

Let a bijection from x to y stand for a bijection between x and y.

Proposition 7.24. Let f be a function from x into y. Then f is a bijection between x and $\mathrm{range}(f)$.

Proof. f is one to one and f is a function from x onto $\mathrm{range}(f)$. Hence f is a bijection between x and $\mathrm{range}(f)$. □

Definition 7.25. A permutation of x is a bijection between x and x.

7.4 The identity function

Let us consider some special function: The *identity* function, which just maps any element of its domain to itself.

Lemma 7.26. There is a function ι of x such that $\iota(u) = u$ for all $u \in x$.

Proof. Define $\iota(u) = u$ for $u \in x$. □

Definition 7.27. id_x is the function of x such that $\mathrm{id}_x(u) = u$ for all $u \in x$.

Let the identity function on x stand for id_x.

Proposition 7.28. id_x is a permutation of x.

Proof. (1) id_x is a function of x.

(2) id_x is a function onto x. Proof. Let $v \in x$. Then $v = \mathrm{id}_x(v)$. Hence $v \in \mathrm{range}(\mathrm{id}_x)$. Qed.

(3) id_x is a function into x. Proof. Let $v, v' \in x$. Assume $\mathrm{id}_x(v) = \mathrm{id}_x(v')$. Then $v = v'$. Qed. □

7.5 Constant functions

Another importat class of functions is that of *constant* functions. Such functions map every element of their domain to the same value.

Lemma 7.29. Let x be a set and v be an element. There is a function c of x such that $c(u) = v$ for all $u \in x$.

Proof. Define $c(u) = v$ for $u \in x$. □

Definition 7.30. $\mathrm{const}_{x,v}$ is the function of x such that $\mathrm{const}_{x,v}(u) = v$ for all $u \in x$.

Let the constant function on x with value v stand for $\mathrm{const}_{x,v}$.

Proposition 7.31. Assume $v \in y$. Then $\mathrm{const}_{x,v}$ is a function from x to y.

Proof. We have $\mathrm{dom}(\mathrm{const}_{x,v}) = x$ and $\mathrm{const}_{x,v}(u) = v$ for all $u \in x$. Hence $\mathrm{const}_{x,v}(u)$ is an element of y for all $u \in x$. Thus $\mathrm{range}(\mathrm{const}_{x,v}) \subseteq y$. Therefore $\mathrm{const}_{x,v}$ is a function from x to y. □

Definition 7.32. Let f be a function. f is constant iff there exists an object v such that $f(u) = v$ for all $u \in \mathrm{dom}(f)$.

Proposition 7.33. $\mathrm{const}_{x,v}$ is constant.

Proof. We have $\mathrm{const}_{x,v}(u) = v$ for all $u \in x$. Hence the thesis. □

7.6 Composition

Let us now consider some operations on functions. The first one, called *composition*, allows us to combine two functions to a new one by applying them one after another.

Lemma 7.34. Assume $\mathrm{range}(f) \subseteq \mathrm{dom}(g)$. Then there is a function h such that $\mathrm{dom}(h) = \mathrm{dom}(f)$ and $h(u) = g(f(u))$ for all $u \in \mathrm{dom}(h)$.

Proof. Define $h(u) = g(f(u))$ for $u \in \mathrm{dom}(f)$. □

Definition 7.35. Assume $\mathrm{range}(f) \subseteq \mathrm{dom}(g)$. $g \circ f$ is the function h such that $\mathrm{dom}(h) = \mathrm{dom}(f)$ and $h(u) = g(f(u))$ for all $u \in \mathrm{dom}(h)$.

Let the composition of g and f stand for $g \circ f$.

Lemma 7.36. Let f be a function from x to y and g be a function from y to z. Then $\mathrm{range}(f) \subseteq \mathrm{dom}(g)$.

Proposition 7.37. Let f be a function from x to y and g be a function from y to z. Then $g \circ f$ is a function from x to z.

Proof. (1) $g \circ f$ is a function of x. Indeed $\mathrm{dom}(g \circ f) = \mathrm{dom}(f) = x$.

(2) $\mathrm{range}(g \circ f) \subseteq z$. Proof. Let $w \in \mathrm{range}(g \circ f)$. Take $u \in x$ such that $(g \circ f)(u) = w$. Then $w = g(f(u))$. We have $f(u) \in y$. Hence $w \in z$. Qed. $\square$

Lemma 7.38. Let f be a function from x to y and g be a function from y to z. Then $\mathrm{dom}(g \circ f) = x$ and $\mathrm{range}(g \circ f) \subseteq z$.

Proposition 7.39. Let f be a function from x to y. Then $f \circ \mathrm{id}_x = f = \mathrm{id}_y \circ f$.

Proof. x is the domain of $f \circ \mathrm{id}_x$ and the domain of f and the domain of $\mathrm{id}_y \circ f$. $(f \circ \mathrm{id}_x)(u) = f(\mathrm{id}_x(u)) = f(u) = \mathrm{id}_y(f(u)) = (\mathrm{id}_y \circ f)(u)$ for all $u \in x$. Hence the thesis (by Function extensionality). $\square$

Proposition 7.40. Let f be a function from x to y and v be an element. Then $\mathrm{const}_{y,v} \circ f = \mathrm{const}_{x,v}$.

Proof. We have $\mathrm{dom}(\mathrm{const}_{y,v} \circ f) = \mathrm{dom}(f) = x = \mathrm{dom}(\mathrm{const}_{x,v})$. $(\mathrm{const}_{y,v} \circ f)(u) = \mathrm{const}_{y,v}(f(u)) = v = \mathrm{const}_{x,v}(u)$ for all $u \in x$. Hence the thesis (by Function extensionality). $\square$

Proposition 7.41. Let f be a function from y to z and $v \in y$. Then $f \circ \mathrm{const}_{x,v} = \mathrm{const}_{x,f(v)}$.

Proof. We have

$$\mathrm{dom}(f \circ \mathrm{const}_{x,v}) = \mathrm{dom}(\mathrm{const}_{x,v}) = x = \mathrm{dom}(\mathrm{const}_{x,f(v)}).$$

For all $u \in x$ we have

$$(f \circ \mathrm{const}_{x,v})(u) = f(\mathrm{const}_{x,v}(u)) = f(v) = \mathrm{const}_{x,f(v)}(u).$$

Hence the thesis (by Function extensionality). $\square$

Proposition 7.42. Let f be a function from x onto y and g be a function from y onto z. Then $g \circ f$ is a function from x onto z.

Proof. $g \circ f$ is a function of x.

Let us show that $g \circ f$ is a function onto z. Let $w \in z$. Take $v \in y$ such that $w = g(v)$. Take $u \in x$ such that $v = f(u)$. Then $w = g(f(u)) = (g \circ f)(u)$. End. $\square$

Proposition 7.43. Let f be a function from x into y and g be a function from y into z. Then $g \circ f$ is a function from x into z.

Proof. $g \circ f$ is a function of x.

Let us show that $g \circ f$ is one to one. Let $u, u' \in x$. Assume $(g \circ f)(u) = (g \circ f)(u')$. Then $g(f(u)) = g(f(u'))$. Hence $f(u) = f(u')$. Indeed $f(u), f(u') \in y$. Thus $u = u'$. End. ☐

Corollary 7.44. Let f be a bijection between x and y and g be a bijection between y and z. Then $g \circ f$ is a bijection between x and z.

Proof. $g \circ f$ is a function from x onto z and a function into z. Hence the thesis. ☐

7.7 Restriction

Another operation on functions is the *restriction* to a subset of their domain.

Lemma 7.45. Let $a \subseteq \mathrm{dom}(f)$. Then there is a function h of a such that $h(u) = f(u)$ for all $u \in a$.

Proof. Define $h(u) = f(u)$ for $u \in a$. ☐

Definition 7.46. Let $a \subseteq \mathrm{dom}(f)$. $f \upharpoonright a$ is the function h of a such that $h(u) = f(u)$ for all $u \in a$.

Let the restriction of f to a stand for $f \upharpoonright a$.

Proposition 7.47. Let f be a function from x to y and $a \subseteq x$. Then $f \upharpoonright a$ is a function from a to y.

Proof. We have $\mathrm{dom}(f \upharpoonright a) = a$. Then $(f \upharpoonright a)(u) = f(u) \in y$ for all $u \in a$. Hence $f \upharpoonright a$ is a function from a to y. ☐

Proposition 7.48. Let $a \subseteq x$. Then $\mathrm{id}_x \upharpoonright a = \mathrm{id}_a$.

Proof. We have $\mathrm{dom}(\mathrm{id}_x \upharpoonright a) = a = \mathrm{dom}(\mathrm{id}_a)$. $(\mathrm{id}_x \upharpoonright a)(u) = \mathrm{id}_x(u) = u = \mathrm{id}_a(u)$ for all $u \in a$. Hence the thesis (by Function extensionality). ☐

Proposition 7.49. Let v be an element and $a \subseteq x$. Then $\mathrm{const}_{x,v} \upharpoonright a = \mathrm{const}_{a,v}$.

Proof. We have $\mathrm{dom}(\mathrm{const}_{x,v} \upharpoonright a) = a = \mathrm{dom}(\mathrm{const}_{a,v})$. $(\mathrm{const}_{x,v} \upharpoonright a)(u) = \mathrm{const}_{x,v}(u) = v = \mathrm{const}_{a,v}(u)$ for all $u \in a$. Hence the thesis (by Function extensionality). ☐

Proposition 7.50. Let f be an one to one function from x to y and $a \subseteq x$. Then $f \upharpoonright a$ is one to one.

Proof. Let $u, u' \in a$. Assume $(f \upharpoonright a)(u) = (f \upharpoonright a)(u')$. Then $f(u) = f(u')$. Hence $u = u'$. ☐

8 Image and preimage

[readtex `set-theory/sections/02_functions/01_functions.ftl.tex`]

Let u, v, w denote objects. Let x, y, z denote sets. Let f, g, h denote functions.

8.1 The image

Given an arbitrary set z we can ask ourselves where its elements are mapped to under a function f. The resulting set of such an application of f to all elements of z is called the *image* of z under f.

Lemma 8.1. Let f be a function. There exists a set y such that $y = \{ f(u) \mid u \in \mathrm{dom}(f) \cap z \}$.

Proof. Take $y = \mathrm{range}(f \restriction (\mathrm{dom}(f) \cap z))$. Then

$$y = \{ (f \restriction (\mathrm{dom}(f) \cap z))(u) \mid u \in \mathrm{dom}(f) \cap z \} .$$

Hence $y = \{ f(u) \mid u \in \mathrm{dom}(f) \cap z \}$. □

Definition 8.2. Let f be a function. $f[z]$ is the set y such that $y = \{ f(u) \mid u \in \mathrm{dom}(f) \cap z \}$.

Let the image of z under f stand for $f[z]$. Let the direct image of z under f stand for $f[z]$.

Proposition 8.3. Let f be a function from x to y and $a \subseteq x$. Then $f[a] = \{ f(u) \mid u \in a \}$.

Proof. $f[a] = \{ f(u) \mid u \in \mathrm{dom}(f) \cap a \}$. $\mathrm{dom}(f) \cap a = x \cap a = a$. Hence the thesis. □

Corollary 8.4. Let f be a function from x to y. Then $f[x] = \mathrm{range}(f)$.

Proof. We have $f[x] = \{ f(u) \mid u \in x \}$. Hence $f[x] = \mathrm{range}(f)$. □

Corollary 8.5. Let f be a function from x to y and $a \subseteq x$. Then $f[a] = \mathrm{range}(f \restriction a)$.

Proof. We have $f[a] = \{ f(u) \mid u \in a \}$. Hence $f[a] = \mathrm{range}(f \restriction a)$. □

Proposition 8.6. Let $a \subseteq x$. Then $\mathrm{id}_x[a] = a$.

Proof. $\mathrm{id}_x[a] = \{ \mathrm{id}_x(u) \mid u \in a \}$. We have $\mathrm{id}_x(u) = u$ for all $u \in a$. Hence $\mathrm{id}_x[a] = \{ u \mid u \in a \}$. Thus $\mathrm{id}_x[a] = a$. □

Proposition 8.7. Let $a \subseteq x$ and v be an element. Assume that a is nonempty. Then $\mathrm{const}_{x,v}[a] = \{v\}$.

Proof. Let us show that $\mathrm{const}_{x,v}[a] \subseteq \{v\}$. Let $w \in \mathrm{const}_{x,v}[a]$. Take $u \in a$ such that $w = \mathrm{const}_{x,v}(u)$. Then $w = v$. Hence $w \in \{v\}$. End.

Let us show that $\{v\} \subseteq \mathrm{const}_{x,v}[a]$. Let $w \in \{v\}$. Then $w = v$. Take $u \in a$. Then $\mathrm{const}_{x,v}(u) = v = w$. Hence $w \in \mathrm{const}_{x,v}[a]$. End. □

Proposition 8.8. Let f be a function from x into y and $a \subseteq x$. Then $f \upharpoonright a$ is a bijection between a and $f[a]$.

Proof. (1) $f \upharpoonright a$ is a function of a.

(2) $f \upharpoonright a$ is one to one.

(3) $\mathrm{range}(f \upharpoonright a) = f[a]$. Proof. Let us show that $\mathrm{range}(f \upharpoonright a) \subseteq f[a]$. Let $v \in \mathrm{range}(f \upharpoonright a)$. Take $u \in a$ such that $v = (f \upharpoonright a)(u)$. Then $v = f(u)$. Hence $v \in f[a]$. End.

Let us show that $f[a] \subseteq \mathrm{range}(f \upharpoonright a)$. Let $v \in f[a]$. Take $u \in a$ such that $v = f(u)$. Then $v = (f \upharpoonright a)(u)$. Hence $v \in \mathrm{range}(f \upharpoonright a)$. End. Qed.

Thus $f \upharpoonright a$ is an one to one function from a onto $f[a]$. Therefore $f \upharpoonright a$ is a bijection between a and $f[a]$. □

8.2 The preimage

Similar to the construction of the image of a set under a function, we can consider a set z and ask ourselves which elements of a function f are mapped into z. This yields the so-called *preimage* of z under f.

Lemma 8.9. Let f be a function. There exists a set y such that $y = \{\, u \in \mathrm{dom}(f) \mid f(u) \in z \,\}$.

Proof. Case $f(u) \in z$ for all $u \in \mathrm{dom}(f)$. Obvious.

Case $f(u) \notin z$ for some $u \in \mathrm{dom}(f)$. Take $w \in \mathrm{dom}(f)$ such that $f(w) \notin z$. (1) Define

$$g(u) = \begin{cases} u & : f(u) \in z \\ w & : f(u) \notin z \end{cases}$$

for $u \in \mathrm{dom}(f)$. $\mathrm{range}(g) = \{\, g(u) \mid u \in \mathrm{dom}(f) \,\}$. Hence $\mathrm{range}(g) = \{\, u \in \mathrm{dom}(f) \mid f(u) \in z \text{ or } u = w \,\}$ (by 1). Take $y = \mathrm{range}(g) \setminus \{w\}$. Then $y = \{\, u \in \mathrm{dom}(f) \mid f(u) \in z \,\}$. End. □

Definition 8.10. Let f be a function. $f^{-}[z]$ is the set y such that $y = \{\, u \in \mathrm{dom}(f) \mid f(u) \in z \,\}$.

Let the preimage of z under f stand for $f^{-}[z]$. Let the inverse image of z under f stand for $f^{-}[z]$.

Proposition 8.11. Let $b \subseteq y$. Then $\mathrm{id}_y^{-}[b] = b$.

Proof. $\mathrm{id}_y^-[b] = \{ u \in y \mid \mathrm{id}_y(u) \in b \}$. $\mathrm{id}_y(u) = u$ for all $u \in y$. Hence $\mathrm{id}_y^-[b] = \{ u \in y \mid u \in b \}$. Thus $\mathrm{id}_y^-[b] = b$. □

Proposition 8.12. Let v be an element and z be a set that contains v. Then $\mathrm{const}_{x,v}^-[z] = x$.

Proof. $\mathrm{const}_{x,v}^-[z] = \{ u \in x \mid \mathrm{const}_{x,v}(u) \in z \}$. $\mathrm{const}_{x,v}(u) = v$ for every $u \in x$. Hence $\mathrm{const}_{x,v}^-[z] = \{ u \in x \mid v \in z \}$. We have $v \in z$. Thus $\mathrm{const}_{x,v}^-[z] = x$. □

Proposition 8.13. Let v be an element and z be a set that does not contain v. Then $\mathrm{const}_{x,v}^-[z] = \emptyset$.

Proof. $\mathrm{const}_{x,v}^-[z] = \{ u \in x \mid \mathrm{const}_{x,v}(u) \in z \}$. $\mathrm{const}_{x,v}(u) = v$ for every $u \in x$. Hence $\mathrm{const}_{x,v}^-[z] = \{ u \in x \mid v \in z \}$. It is wrong that $v \in z$. Thus $\mathrm{const}_{x,v}^-[z] = \emptyset$. □

8.3 Computation rules

To conclude this paragraph let us prove some facts about the image and preimage.

Proposition 8.14. Let f be a function from x to y and $a \subseteq x$ and $u \in x$. Then $u \in a \implies f(u) \in f[a]$.

Proof. Assume $u \in a$. We have $f[a] = \{ f(u') \mid u' \in a \}$. Hence $f(u) \in f[a]$. □

Proposition 8.15. Let f be a function from x to y and $b \subseteq y$ and $u \in x$. Then $f(u) \in b \iff u \in f^-[b]$.

Proof. We have $f^-[b] = \{ u' \in x \mid f(u') \in b \}$. Hence $u \in f^-[b]$ iff $u \in x$ and $f(u) \in b$. Then we have the thesis. □

Proposition 8.16. Let f be a function from x to y. Then $f[x] \subseteq y$.

Proof. $f[x] = f[\mathrm{dom}(f)] = \mathrm{range}(f) \subseteq y$. □

Proposition 8.17. Let f be a function from x to y. Then $f^-[y] = x$.

Proof. We have $f^-[y] = \{ u \in x \mid f(u) \in y \}$. $f(u)$ is an element of y for all $u \in x$. Hence the thesis. □

Proposition 8.18. Let f be a function from x to y. Then $f[f^-[y]] = f[x]$.

Proof. Let us show that $f[f^-[y]] \subseteq f[x]$. Let $v \in f[f^-[y]]$. Take $u \in f^-[y] \cap x$ such that $v = f(u)$. Then $u \in x$. Hence $v \in f[x]$. End.

Let us show that $f[x] \subseteq f[f^{-}[y]]$. Let $v \in f[x]$. Take $u \in x$ such that $v = f(u)$. We have $v \in y$. Hence $u \in f^{-}[y]$. Thus $f(u) \in f[f^{-}[y]]$. Indeed $f^{-}[y] \subseteq x$. Therefore $v \in f[f^{-}[y]]$. End. $\square$

Proposition 8.19. Let f be a function from x to y. Then $f^{-}[f[x]] = x$.

Proof. $f^{-}[f[x]] = \{ u \in x \mid f(u) \in f[x] \}$. For all $u \in x$ we have $f(u) \in f[x]$. Hence every element of $f^{-}[f[x]]$ is contained in x and every element of x is contained in $f^{-}[f[x]]$. Thus $f^{-}[f[x]] = x$. $\square$

Proposition 8.20. Let f be a function from x to y and $b \subseteq y$. Then $f[f^{-}[b]] = b \cap f[x]$.

Proof. Let us show that $f[f^{-}[b]] \subseteq b \cap f[x]$. Let $v \in f[f^{-}[b]]$. Take $u \in f^{-}[b]$ such that $v = f(u)$. Then $f(u) \in b \cap f[x]$. Hence we have $v \in b \cap f[x]$. End.

Let us show that $b \cap f[x] \subseteq f[f^{-}[b]]$. Let $v \in b \cap f[x]$. Take $u \in x$ such that $v = f(u)$. Then $u \in f^{-}[b]$. Hence $f(u) \in f[f^{-}[b]]$. End. $\square$

Corollary 8.21. Let f be a function from x to y and $b \subseteq y$. Then $f[f^{-}[b]] \subseteq b$.

Proof. We have $f[f^{-}[b]] = b \cap f[x] \subseteq b$. Hence $f[f^{-}[b]] \subseteq b$. $\square$

Proposition 8.22. Let f be a function from x to y and $a \subseteq x$. Then $f^{-}[f[a]] \supseteq a$.

Proof. Let $u \in a$. Then $f(u) \in f[a]$. Hence $u \in f^{-}[f[a]]$. Indeed $f[a] \subseteq y$. $\square$

Proposition 8.23. Let f be a function from x to y and $a \subseteq x$. Then $f[a] = \emptyset \iff a = \emptyset$.

Proof. Case $f[a] = \emptyset$. Then there is no $u \in a$ such that $f(u) \in f[a]$. For all $u \in a$ we have $f(u) \in f[a]$. Hence a is empty. End.

Case $a = \emptyset$. For all $v \in f[a]$ we have $v = f(u)$ for some $u \in a$. There is no $u \in a$. Hence $f[a]$ is empty. End. $\square$

Proposition 8.24. Let f be a function from x to y and $b \subseteq y$. Then $f^{-}[b] = \emptyset \iff b \subseteq y \setminus f[x]$.

Proof. Case $f^{-}[b] = \emptyset$. Let $v \in b$. Then $v \in y$.

There is no $u \in x$ such that $v = f(u)$.
Proof. Assume the contrary. Take $u \in x$ such that $v = f(u)$. Then $u \in f^{-}[b]$. Contradiction. Qed.

Hence $v \notin f[x]$. Therefore $v \in y \setminus f[x]$. End.

Case $b \subseteq y \setminus f[x]$. Then no element of b is an element of $f[x]$. Assume that $f^{-}[b]$ is nonempty. Take $u \in f^{-}[b]$. Then $f(u) \in b$ and $f(u) \in f[x]$. Contradiction. End. ☐

Proposition 8.25. Let f be a function from x to y and $a \subseteq x$ and $b \subseteq y$. Then $f[a] \cap b = \emptyset \iff a \cap f^{-}[b] = \emptyset$.

Proof. Case $f[a] \cap b = \emptyset$. Assume that $a \cap f^{-}[b]$ is nonempty. Take $u \in a \cap f^{-}[b]$. Then $f(u) \in f[a]$ and $f(u) \in b$. Hence $f(u) \in f[a] \cap b$. Contradiction. End.

Case $a \cap f^{-}[b] = \emptyset$. Assume that $f[a] \cap b$ is nonempty. Take $v \in f[a] \cap b$. Consider a $u \in a$ such that $v = f(u)$. Then $u \in f^{-}[b]$. Indeed $v \in b$. Hence $u \in a \cap f^{-}[b]$. Contradiction. End. ☐

Proposition 8.26. Let f be a function from x to y and g be a function from y to z and $a \subseteq x$. Then $(g \circ f)[a] = g[f[a]]$.

Proof. $((g \circ f)[a]) = \{ g(f(u)) \mid u \in a \}$. $f[a]$ is a subset of y. We have $g[f[a]] = \{ g(v) \mid v \in f[a] \}$ and $f[a] = \{ f(u) \mid u \in a \}$. Thus $g[f[a]] = \{ g(f(u)) \mid u \in a \}$. Therefore $(g \circ f)[a] = g[f[a]]$. Indeed $((g \circ f)[a])$ and $g[f[a]]$ are sets. ☐

Proposition 8.27. Let f be a function from x to y and g be a function from y to z and $c \subseteq z$. Then $(g \circ f)^{-}[z] = f^{-}[g^{-}[z]]$.

Proof. $((g \circ f)^{-}[z]) = \{ u \in x \mid g(f(u)) \in z \}$. We have $g^{-}[z] = \{ v \in y \mid g(v) \in z \}$ and $f^{-}[g^{-}[z]] = \{ u \in x \mid f(u) \in g^{-}[z] \}$. Hence $f^{-}[g^{-}[z]] = \{ u \in x \mid g(f(u)) \in z \}$. Thus $(g \circ f)^{-}[z] = f^{-}[g^{-}[z]]$. ☐

Proposition 8.28. Let f be a function from x to y and $a, a' \subseteq x$. Then $a \subseteq a' \implies f[a] \subseteq f[a']$.

Proof. Assume $a \subseteq a'$. Let $v \in f[a]$. Take $u \in a$ such that $f(u) = v$. Then $u \in a'$. Hence $v = f(u) \in f[a']$. ☐

Proposition 8.29. Let f be a function from x to y and $b, b' \subseteq y$. Then $b \subseteq b' \implies f^{-}[b] \subseteq f^{-}[b']$.

Proof. Assume $b \subseteq b'$. Let $u \in f^{-}[b]$. Then $f(u) \in b$. Hence $f(u) \in b'$. Thus $u \in f^{-}[b']$. ☐

Proposition 8.30. Let f be a function from x to y and $a, a' \subseteq x$. Then $f[a \cup a'] = f[a] \cup f[a']$.

Proof. Let us show that $f[a \cup a'] \subseteq f[a] \cup f[a']$. Let $v \in f[a \cup a']$. Take $u \in a \cup a'$ such that $v = f(u)$. Then $u \in a$ or $u \in a'$. Hence $f(u) \in f[a]$ or $f(u) \in f[a']$. Thus $v = f(u) \in f[a] \cup f[a']$. End.

Let us show that $f[a] \cup f[a'] \subseteq f[a \cup a']$. Let $v \in f[a] \cup f[a']$.

Case $v \in f[a]$. Take $u \in a$ such that $v = f(u)$. Then $u \in a \cup a'$. Hence $v \in f[a \cup a']$. End.

Case $v \in f[a']$. Take $u \in a'$ such that $v = f(u)$. Then $u \in a \cup a'$. Hence $v \in f[a \cup a']$. End. End. $\square$

Proposition 8.31. Let f be a function from x to y and $b, b' \subseteq y$. Then $f^-[b \cup b'] = f^-[b] \cup f^-[b']$.

Proof. Let us show that $f^-[b \cup b'] \subseteq f^-[b] \cup f^-[b']$. Let $u \in f^-[b \cup b']$. Then $f(u) \in b \cup b'$. Hence $f(u) \in b$ or $f(u) \in b'$. If $f(u) \in b$ then $u \in f^-[b]$. If $f(u) \in b'$ then $u \in f^-[b']$. Thus $u \in f^-[b] \cup f^-[b']$. End.

Let us show that $f^-[b] \cup f^-[b'] \subseteq f^-[b \cup b']$. Let $u \in f^-[b] \cup f^-[b']$. Then $u \in f^-[b]$ or $u \in f^-[b']$. If $u \in f^-[b]$ then $f(u) \in b$. If $u \in f^-[b']$ then $f(u) \in b'$. Hence $f(u) \in b \cup b'$. Thus $u \in f^-[b \cup b']$. End. $\square$

Proposition 8.32. Let f be a function from x to y and $a, a' \subseteq x$. Then $f[a \cap a'] \subseteq f[a] \cap f[a']$.

Proof. Let $v \in f[a \cap a']$. Take $u \in a \cap a'$ such that $v = f(u)$. Then $u \in a$ and $u \in a'$. Hence $f(u) \in f[a]$ and $f(u) \in f[a']$. Thus $v \in f[a] \cap f[a]$. $\square$

Proposition 8.33. Let f be a function from x to y and $b, b' \subseteq y$. Then $f^-[b \cap b'] = f^-[b] \cap f^-[b']$.

Proof. Let us show that $f^-[b \cap b'] \subseteq f^-[b] \cap f^-[b']$. Let $u \in f^-[b \cap b']$. Then $f(u) \in b \cap b'$. Hence $f(u) \in b$ and $f(u) \in b'$. Thus $u \in f^-[b]$ and $u \in f^-[b']$. Therefore $u \in f^-[b] \cap f^-[b']$. End.

Let us show that $f^-[b] \cap f^-[b'] \subseteq f^-[b \cap b']$. Let $u \in f^-[b] \cap f^-[b']$. Then $u \in f^-[b]$ and $u \in f^-[b']$. Hence $f(u) \in b$ and $f(u) \in b'$. Thus $f(u) \in b \cap b'$. Therefore $u \in f^-[b \cap b']$. End. $\square$

Proposition 8.34. Let f be a function from x to y and $a, a' \subseteq x$. Then $f[a \setminus a'] \supseteq f[a] \setminus f[a']$.

Proof. Let $v \in f[a] \setminus f[a']$. Then $v \in f[a]$ and $v \notin f[a']$. Take $u \in a$ such that $v = f(u)$. If $u \in a'$ then $v \in f[a']$. Hence $u \notin a'$. Thus $u \in a \setminus a'$. Therefore $v = f(u) \in f[a \setminus a']$. $\square$

Proposition 8.35. Let f be a function from x to y and $b, b' \subseteq y$. Then $f^-[b \setminus b'] = f^-[b] \setminus f^-[b']$.

Proof. Let us show that $f^-[b \setminus b'] \subseteq f^-[b] \setminus f^-[b']$. Let $u \in f^-[b \setminus b']$. Then $f(u) \in b \setminus b'$. Hence $f(u) \in b$ and $f(u) \notin b'$. Thus $u \in f^-[b]$ and $u \notin f^-[b']$. Therefore $u \in f^-[b] \setminus f^-[b']$. End.

Let us show that $f^-[b] \setminus f^-[b'] \subseteq f^-[b \setminus b']$. Let $u \in f^-[b] \setminus f^-[b']$. Then $u \in f^-[b]$ and $u \notin f^-[b']$. Hence $f(u) \in b$ and $f(u) \notin b'$. Thus $f(u) \in b \setminus b'$. Therefore $u \in f^-[b \setminus b']$. End. $\square$

9 Invertible functions

[readtex `set-theory/sections/02_functions/02_image-and-preimage.ftl.tex`]

Let u, v, w denote objects. Let x, y, z denote sets. Let f, g, h denote functions.

9.1 Definitions and basic properties

We call a function f *invertible* if there is a function g that undoes the operation of f, i.e. applying f after g and applying g after f each results in the identity function.

Definition 9.1. An inverse of f is a function g from $\mathrm{range}(f)$ to $\mathrm{dom}(f)$ such that

$$f(u) = v \iff g(v) = u$$

for all $u \in \mathrm{dom}(f)$ and all $v \in \mathrm{dom}(g)$.

Definition 9.2. f is invertible iff f has an inverse.

Lemma 9.3. Let g, g' be inverses of f. Then $g = g'$.

Proof. We have $\mathrm{dom}(g) = \mathrm{range}(f) = \mathrm{dom}(g')$.

Let us show that $g(v) = g'(v)$ for all $v \in \mathrm{range}(f)$. Let $v \in \mathrm{range}(f)$. Take $u = g'(v)$. Then $g(v) = u$ iff $f(u) = v$. We have $f(u) = v$ iff $g'(v) = u$. Thus $g(v) = g'(v)$. End.

Hence the thesis (by Function extensionality). Indeed $\mathrm{dom}(g) = \mathrm{dom}(g')$. ☐

Definition 9.4. Let f be invertible. f^{-1} is the inverse of f.

Let f is involutory stand for f is the inverse of f. Let f is selfinverse stand for f is the inverse of f.

Proposition 9.5. Let f be a function from x onto y and g be a function from y onto x. Then g is the inverse of f iff $g \circ f = \mathrm{id}_x$ and $f \circ g = \mathrm{id}_y$.

Proof. Case g is the inverse of f. We have $\mathrm{dom}(g \circ f) = \mathrm{dom}(f) = x = \mathrm{dom}(\mathrm{id}_x)$. For all $u \in x$ we have $(g \circ f)(u) = g(f(u)) = u$. Hence $g \circ f = \mathrm{id}_x$.

We have $\mathrm{dom}(f \circ g) = \mathrm{dom}(g) = y = \mathrm{dom}(\mathrm{id}_y)$. For all $v \in y$ we have $(f \circ g)(v) = f(g(v)) = v$. Hence $f \circ g = \mathrm{id}_y$. End.

Case $g \circ f = \mathrm{id}_x$ and $f \circ g = \mathrm{id}_y$. Then $\mathrm{dom}(g) = y = \mathrm{range}(f)$ and $\mathrm{range}(g) = x = \mathrm{dom}(f)$. Let $u \in \mathrm{dom}(f)$ and $v \in \mathrm{dom}(g)$. If $f(u) = v$ then $g(v) = g(f(u)) = (g \circ f)(u) = \mathrm{id}_x(u) = u$. If $g(v) = u$ then $f(u) = f(g(v)) = (f \circ g)(v) = \mathrm{id}_y(v) = v$. Hence $f(u) = v$ iff $g(v) = u$. End. ☐

Proposition 9.6. Let f be an invertible function from x onto y. Then f^{-1} is an invertible function from y onto x such that $(f^{-1})^{-1} = f$.

Proof. f^{-1} is a function from y to x. Indeed $\mathrm{range}(f) = y$ and $\mathrm{dom}(f) = x$. f^{-1} is a function onto x. Indeed for any $u \in x$ we have $f^{-1}(f(u)) = u$. f^{-1} is the inverse of f. Thus $f \circ f^{-1} = \mathrm{id}_y$ and $f^{-1} \circ f = \mathrm{id}_x$. Therefore f is the inverse of f^{-1} (by 9.5). □

Proposition 9.7. Let f be an invertible function from x onto y. Then $f \circ f^{-1} = \mathrm{id}_y$ and $f^{-1} \circ f = \mathrm{id}_x$.

Proof. f^{-1} is a function from y onto x (by 9.6). f^{-1} is the inverse of f. Hence the thesis (by 9.5). □

Proposition 9.8. Let f be an invertible function from x onto y. Then ($f^{-1}(f(u)) = u$ for all $u \in x$) and ($f(f^{-1}(v)) = v$ for all $v \in y$).

Proof. Let us show that $f^{-1}(f(u)) = u$ for all $u \in x$. Let $u \in x$. Then $f^{-1}(f(u)) = (f^{-1} \circ f)(u) = \mathrm{id}_x(u) = u$. End.

Let us show that $f(f^{-1}(v)) = v$ for all $v \in y$. Let $v \in y$. Then $f(f^{-1}(v)) = (f \circ f^{-1})(v) = \mathrm{id}_y(v) = v$. End. □

Proposition 9.9. Let f be an invertible function from x onto y and g be an invertible function from y onto z. Then $g \circ f$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. f^{-1} is a function from y onto x. g^{-1} is a function from z onto y. Take $h = f^{-1} \circ g^{-1}$. [prover vampire] Then h is a function from z onto x (by 7.42). [prover eprover] $g \circ f$ is a function from x to z.

Let us show that $((g \circ f) \circ h) = \mathrm{id}_z$. We have $f \circ (f^{-1} \circ g^{-1}) = (f \circ f^{-1}) \circ g^{-1}$ (by Function extensionality). Indeed $f \circ (f^{-1} \circ g^{-1})$ and $(f \circ f^{-1}) \circ g^{-1}$ are functions of z. $f \circ h$ is a function from z to y. Hence

$$
\begin{aligned}
&(g \circ f) \circ h \\
&= g \circ (f \circ h) \\
&= g \circ (f \circ (f^{-1} \circ g^{-1})) \\
&= g \circ ((f \circ f^{-1}) \circ g^{-1}) \\
&= g \circ (\mathrm{id}_y \circ g^{-1}) \\
&= g \circ g^{-1} \\
&= \mathrm{id}_z \,.
\end{aligned}
$$

End.

Let us show that $h \circ (g \circ f) = \mathrm{id}_x$. We have $(f^{-1} \circ g^{-1}) \circ g = f^{-1} \circ (g^{-1} \circ g)$ (by Function extensionality). $g \circ f$ is a function from x to z. Hence

$$\begin{aligned} & h \circ (g \circ f) \\ &= (h \circ g) \circ f \\ &= ((f^{-1} \circ g^{-1}) \circ g) \circ f \\ &= (f^{-1} \circ (g^{-1} \circ g)) \circ f \\ &= (f^{-1} \circ \mathrm{id}_y) \circ f \\ &= f^{-1} \circ f \\ &= \mathrm{id}_x . \end{aligned}$$

End.

Thus h is the inverse of $g \circ f$ (by 9.5). Indeed $g \circ f$ is a function from x onto z and h is a function from z onto x. □

Proposition 9.10. Let f be an invertible function from x onto y and $a \subseteq x$. Then $f \restriction a$ is invertible and $(f \restriction a)^{-1} = f^{-1} \restriction f[a]$.

Proof. $f \restriction a$ is a function from a onto $f[a]$. Take $g = f^{-1} \restriction f[a]$. Then g is a function of $f[a]$.

Let us show that $a \subseteq \mathrm{range}(g)$. Let $u \in a$. Then $f(u) \in f[a]$. Hence $g(f(u)) = f^{-1}(f(u)) = u$. Thus u is a value of g. End.

Let us show that $\mathrm{range}(g) \subseteq a$. Let $u \in \mathrm{range}(g)$. Take $v \in f[a]$ such that $u = g(v)$. Take $w \in a$ such that $v = f(w)$. Then $u = (f^{-1} \restriction f[a])(v) = f^{-1}(v) = f^{-1}(f(w)) = w$. Hence $u \in a$. End.

Hence $\mathrm{range}(g) = a$. Thus g is a function onto a.

Let us show that $g((f \restriction a)(u)) = u$ for all $u \in a$. Let $u \in a$. Then $g((f \restriction a)(u)) = g(f(u)) = (f^{-1} \restriction f[a])(f(u)) = f^{-1}(f(u)) = u$. End.

Let us show that $((f \restriction a)(g(v))) = v$ for all $v \in f[a]$. Let $v \in f[a]$. Take $u \in a$ such that $v = f(u)$. We have $g(v) = g(f(u)) = (f^{-1} \restriction f[a])(f(u)) = f^{-1}(f(u)) = u$. Hence $(f \restriction a)(g(v)) = (f \restriction a)(u) = f(u) = v$. End.

Thus $g \circ (f \restriction a) = \mathrm{id}_a$ and $(f \restriction a) \circ g = \mathrm{id}_{f[a]}$. Therefore g is the inverse of $f \restriction a$. □

Proposition 9.11. Let f be an invertible function from x onto y and $b \subseteq y$. Then $f^{-}[b] = f^{-1}[b]$.

Proof. We have $f^{-1}[b] = \left\{ f^{-1}(v) \,\middle|\, v \in b \right\}$ and $f^{-}[b] = \{ u \in x \mid f(u) \in b \}$.

Let us show that $f^{-}[b] \subseteq f^{-1}[b]$. Let $u \in f^{-}[b]$. Take $v \in b$ such that $v = f(u)$. Then $f^{-1}(v) = f^{-1}(f(u)) = u$. Hence $u \in f^{-1}[b]$. End.

Let us show that $f^{-1}[b] \subseteq f^{-}[b]$. Let $u \in f^{-1}[b]$. Take $v \in b$ such that $u = f^{-1}(v)$. Then $f(u) = f(f^{-1}(v)) = v$. Hence $u \in f^{-}[b]$. End. $\square$

Corollary 9.12. Let f be an invertible function from x onto y and $v \in y$. Then $f^{-}[\{v\}] = \{f^{-1}(v)\}$.

Proof. $f^{-}[\{v\}] = f^{-1}[\{v\}]$. We have $f^{-1}[\{v\}] = \left\{ f^{-1}(w) \;\middle|\; w \in \{v\} \right\}$. Hence $f^{-1}[\{v\}] = \{f^{-1}(v)\}$. $\square$

Proposition 9.13. Let f be a function from x onto y. f is invertible iff f is one to one.

Proof. Case f is invertible. Let $u, v \in x$. Assume $f(u) = f(v)$. Then $u = f^{-1}(f(u)) = f^{-1}(f(v)) = v$. End.

Case f is one to one. Define $g(v) =$ choose $u \in x$ such that $f(u) = v$ in u for $v \in y$. g is a function from y to x. For all $v \in y$ and all $u, u' \in x$ such that $f(u) = v = f(u')$ we have $u = u'$. Hence g is a function from y onto x. For all $u \in x$ we have $g(f(u)) = u$. For all $v \in y$ we have $f(g(v)) = v$. Hence g is the inverse of f. End. $\square$

Corollary 9.14. Let f be an invertible function from x onto y. Then f^{-1} is a bijection between y and x.

Proof. f^{-1} is a function from y onto x. f^{-1} is invertible. Hence f^{-1} is one to one. Thus f^{-1} is a function from y into x. Therefore f^{-1} is a bijection between y and x. $\square$

9.2 Involutions

A special case of invertible functions are *involutions*, i.e. functions which are self-inverse on their domain.

Definition 9.15. An involution on x is a selfinverse function f on x.

Proposition 9.16. id_x is an involution on x.

Proof. id_x is a function on x. We have $\mathrm{id}_x \circ \mathrm{id}_x = \mathrm{id}_x$. Hence id_x is selfinverse. $\square$

Proposition 9.17. Let f and g be involutions on x. Then $g \circ f$ is an involution on x iff $g \circ f = f \circ g$.

Proof. Case $g \circ f$ is an involution on x. Then $(g \circ f)^{-1} = f^{-1} \circ g^{-1} = f \circ g$. End.

Case $g \circ f = f \circ g$. $f \circ f$, $f \circ g$ and $f \circ g$ are functions on x. Hence

$$(g \circ f) \circ (g \circ f)$$

$$
\begin{aligned}
&= (g \circ f) \circ (f \circ g) \\
&= ((g \circ f) \circ f) \circ g \\
&= (g \circ (f \circ f)) \circ g \\
&= (g \circ \mathrm{id}_x) \circ g \\
&= g \circ g \\
&= \mathrm{id}_x .
\end{aligned}
$$

Thus $g \circ f$ is selfinverse. End. □

Corollary 9.18. Let f be an involutions on x. Then $f \circ f$ is an involution on x.

Proposition 9.19. Let f be an involution on x. Then f is a permutation of x.

Proof. f is an invertible function from x onto x. Hence f is a bijection between x and x. Thus f is a permutation of x. □

10 Functions and the symmetric difference

[readtex `set-theory/sections/01_sets/04_symmetric-difference.ftl.tex`]

[readtex `set-theory/sections/02_functions/02_image-and-preimage.ftl.tex`]

Let u, v, w denote objects. Let x, y, z denote sets. Let f, g, h denote functions.

In this paragraph we will briefly examine the behaviour of the image and preimage of a function with respect to the symmetric difference.

Proposition 10.1. Let f be a function from x to y and $a, a' \subseteq x$. Then

$$f[a \triangle a'] \supseteq f[a] \triangle f[a'].$$

Proof. Let $v \in f[a] \triangle f[a']$. We have $f[a] \triangle f[a'] = (f[a] \cup f[a']) \setminus (f[a] \cap f[a'])$. Hence $v \in f[a] \cup f[a']$ and $v \notin f[a] \cap f[a']$. We have $f[a] \cup f[a'] = f[a \cup a']$ (by 8.30).

Thus we can take $u \in a \cup a'$ such that $v = f(u)$.

Let us show that $u \notin a \cap a'$. Assume the contrary. Then $v = f(u) \in f[a \cap a']$. We have $f[a \cap a'] \subseteq f[a] \cap f[a']$. Hence $v \in f[a] \cap f[a']$. Contradiction. End.

Thus $u \in a \triangle a'$. Therefore $v \in f[a \triangle a']$. □

Proposition 10.2. Let f be a function from x to y and $b, b' \subseteq y$. Then

$$f^-[b \triangle b'] \supseteq f^-[b] \triangle f^-[b'].$$

Proof. Let $u \in f^-[b] \triangle f^-[b']$. Then $u \in f^-[b] \cup f^-[b']$ and $u \notin f^-[b] \cap f^-[b']$. We have $f^-[b] \cup f^-[b'] = f^-[b \cup b']$. Hence we can take $v \in b \cup b'$ such that $f(u) = v$.

Let us show that $v \notin b \cap b'$. Assume the contrary. Then $v = f(u) \in b \cap b'$. Hence $u \in f^-[b \cap b'] = f^-[b] \cap f^-[b']$. Contradiction. End.

Therefore $v \in b \triangle b'$. Hence $u \in f^-[b \triangle b']$. □

11 Functions and set-systems

[readtex `set-theory/sections/01_sets/02_powerset.ftl.tex`]

[readtex `set-theory/sections/02_functions/01_functions.ftl.tex`]

Let u, v, w denote objects. Let x, y, z denote sets. Let f, g, h denote functions.

When dealing with set-systems, we might want to consider functions wich preserve the order given by the $\subseteq$-relation on these set-systems.

Definition 11.1. A function between systems of sets is a function f such that f is a function from X to Y for some systems of sets X, Y.

Definition 11.2. Let f be a function between systems of sets. f preserves subsets iff for all $x, y \in \mathrm{dom}(f)$ if $x \subseteq y$ then $f(x) \subseteq f(y)$.

Definition 11.3. Let f be a function between systems of sets. f preserves supersets iff for all $x, y \in \mathrm{dom}(f)$ if $x \supseteq y$ then $f(x) \supseteq f(y)$.

Lemma 11.4. Let f be a function between systems of sets. Then f preserves subsets iff f preserves supersets.

Proof. Case f preserves subsets. Let $x, y \in \mathrm{dom}(f)$. Assume $x \supseteq y$. Then $y \subseteq x$. Hence $f(y) \subseteq f(x)$. Thus $f(x) \supseteq f(y)$. End.

Case f preserves supersets. Let $x, y \in \mathrm{dom}(f)$. Assume $x \subseteq y$. Then $y \supseteq x$. Hence $f(y) \supseteq f(x)$. Thus $f(x) \subseteq f(y)$. End. □

A famous result about order-preserving functions is the *Knaster-Tarski fixed point theorem*:

Theorem 11.5 (Knaster-Tarski). Let h be a function from $\mathcal{P}(x)$ to $\mathcal{P}(x)$ that preserves subsets. Then h has a fixed point.

Proof. (1) Define $A = \{ y \mid y \subseteq x \text{ and } y \subseteq h(y) \}$. Then A is a subset of $\mathcal{P}(x)$ (by Separation). We have $\bigcup A \in \mathcal{P}(x)$.

Let us show that (2) $\bigcup A \subseteq h(\bigcup A)$. Let $u \in \bigcup A$. Take $y \in A$ such that $u \in y$. Then $u \in h(y)$. We have $y \subseteq \bigcup A$. Hence $h(y) \subseteq h(\bigcup A)$. Thus $h(y) \subseteq h(\bigcup A)$. Therefore $u \in h(\bigcup A)$. End.

Then $h(\bigcup A) \in A$ (by 1). Indeed $h(\bigcup A) \subseteq x$. (3) Hence $h(\bigcup A) \subseteq \bigcup A$. Indeed every element of $h(\bigcup A)$ is an element of some element of A.

Thus $h(\bigcup A) = \bigcup A$ (by 2, 3). □

12 Equipollency

[readtex `set-theory/sections/02_functions/03_invertible-functions.ftl.tex`]

Let u, v, w denote objects. Let x, y, z denote sets. Let f, g, h denote functions.

We conclude this part about functions by introducing the notion of *equipollency*: Two sets x, y being equipollent expresses the idea of x and y having the same number of elements.

Definition 12.1. x and y are equipollent iff there exists a bijection between x and y.

Let x and y are equipotent stand for x and y are equipollent.

Proposition 12.2. x and x are equipollent.

Proof. id_x is a bijection between x and x. □

Proposition 12.3. If x and y are equipollent then y and x are equipollent.

Proof. Assume that x and y are equipollent. Take a bijection f between x and y. Then f^{-1} is a bijection between y and x. Hence y and x are equipollent. □

Proposition 12.4. If x and y are equipollent and y and z are equipollent then x and z are equipollent.

Proof. Assume that x and y are equipollent and y and z are equipollent. Take a bijection f between x and y. Take a bijection g between y and z. Then $g \circ f$ is a bijection between x and z. Hence x and z are equipollent. □

Proposition 12.5. x and $\emptyset$ are equipollent iff x is empty.

Proof. Case x and $\emptyset$ are equipollent. Take a bijection f between x and $\emptyset$. Assume that x is nonempty. Take an element u of x. Then $f(u) \in \emptyset$. Contradiction. End.

Case x is empty. Then $x = \emptyset$. Hence x and $\emptyset$ are equipollent. End. $\square$