Analysis

Marc Mertens

Email: marc.lisp@gmail.com

June 3, 2023

Chapter 1
Elements of set theory

1.1 Basic concepts about classes and sets

Every book about mathematical subjects must be based on one form of set theory. Because the focus of this book is on mathematical analysis instead of the foundations of mathematics, I have decided to use Von Neumann's set theory instead of the set theory of Fraenkel, Skolem and Zermelo. The benefit of Von Neumann's theory is that it is nearer to the naive set theory of Cantor. This book assumes that the basics of mathematical logic are understood, more specifically that the reader knows the meaning of the following terms:

$$\begin{array}{rll}\wedge & \text{meaning} & \text{and}\\ \vee & \text{meaning} & \text{or}\\ \neg & \text{meaning} & \text{not}\\ \Rightarrow & \text{meaning} & \text{implies}\\ \Leftrightarrow & \text{meaning} & \text{is equivalent with}\\ \vdash,\vDash & \text{meaning} & \text{with, where}\\ \forall & \text{meaning} & \text{for all}\\ \exists & \text{meaning} & \text{there exists}\\ \exists! & \text{meaning} & \text{there exists } a \text{ unique}\end{array}$$

and how to use them. Axiomatic set theory is based on two undefined concepts: **class** and the **membership** relation between classes (noted as $\in$). Intuitive you can think of a class as a collection and $x \in A$ to mean that x is part of the collection where A stands for. We introduce then axioms that state which are true statements about these undefined concepts. Further we introduce different definitions that helps us to simplify our notation. To start with, we define the concept of $\notin$ [not member of]

Definition 1.1. *Let A be a class then $x \notin A$ is equivalent with saying $\neg(x \in A)$.*

Next we define **sets** and **elements**, they are the same thing. A **set** or **element** is something that is a member of a class.

Definition 1.2. *We say that a **class** x is a **element** if $x \in A$ where A is a class. Another name for a **element** is a **set***

From here on we use the following convention: elements are noted in **lower-case** and classes are noted in **upper-case**. Next we define equality of classes.

Definition 1.3. *Let A, B classes then we say that $A = B$ if and only if*

$$\forall X \text{ we have } A \in X \Rightarrow B \in X \wedge B \in X \Rightarrow A \in X$$

Less formally, two classes A and B are equal if every class that contains A or B must contains B or A.

Once we have defined equality we can define inequality

Definition 1.4. *Let A and B classes then $A \neq B$ is equivalent with $\neg(A = B)$*

If two classes are equal, we expect them to contain the same elements, this is stated in the first set axiom.

Axiom 1.5. (Axiom of extent)

$$A = B \Leftrightarrow [x \in A \Rightarrow x \in B \wedge x \in B \Rightarrow x \in A]$$

Less formally A is equal to B if and only if ever element of A is a element of B and every element of B is a element of A, in other words A and B have the same elements.

Definition 1.6. *Let A and B classes then A is a sub-class of B noted by $A \subseteq B$ iff*

$$x \in A \Rightarrow x \in B$$

So A is a sub-class of B iff every element of A is also a element of B.

Definition 1.7. *Let A and B classes then A is a proper sub-class of B noted by $A \subsetneq B$ iff*

$$x \in A \Rightarrow x \in B \wedge A \neq B$$

So A is a proper sub-class of B iff A is different from B and every element of A is also a element of B.

Theorem 1.8. *Let A, B, C be classes then the following holds:*

1. $A = A$
2. $A = B \Rightarrow B = A$
3. $A = B \wedge B = C \Rightarrow A = C$
4. $A \subseteq B \wedge B \subseteq A \Rightarrow A = B$
5. $A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$
6. $A = B \Rightarrow A \subseteq B$

Proof.

1. $x \in A \Rightarrow x \in A$ and $x \in A \Rightarrow x \in A$ are obviously true, hence using the Axiom of Extent [axiom: 1.5] it follows that $A = A$
2. As $A = B$ we have using the Axiom of Extent [axiom: 1.5] that $x \in A \Rightarrow x \in B \wedge x \in B \Rightarrow x \in A$ which is equivalent with $x \in B \Rightarrow x \in A \wedge x \in A \Rightarrow x \in B$. Using the Axiom of Extent [axiom: 1.5] it follows that $B = A$
3. As $A = B \wedge B = A$ we have by he Axiom of Extent [axiom: 1.5] that
$$x \in A \Rightarrow x \in B \tag{1.1}$$
$$x \in B \Rightarrow x \in A \tag{1.2}$$
$$x \in B \Rightarrow x \in C \tag{1.3}$$
$$x \in C \Rightarrow x \in B \tag{1.4}$$
From [eq: 1.1] and [eq: 1.3] it follows that $x \in A \Rightarrow x \in C$ and from [eq: 1.4] and [eq: 1.2] it follows that $x \in C \Rightarrow x \in A$. Using the Axiom of Extent [axiom: 1.5] it follows then that $A = C$.
4. From $A \subseteq B \wedge B \subseteq A$ it follows that $x \in A \Rightarrow x \in B \wedge x \in B \Rightarrow x \in A$, so by the Axiom of Extent [axiom: 1.5] we have $A = b$
5. As $A \subseteq B \wedge B \subseteq C$ that $x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in C$ proving that $x \in A \Rightarrow x \in C$ or $A \subseteq C$
6. If $x \in A$ then as $A = B$ we have by the axiom of extension [axiom: 1.5] that $x \in B$, hence $A \subseteq B$.

$\square$

One way to create a new class is to specify a predicate that a object must satisfies and then take the class of all objects that satisfies this predicate. The problem with this construction is that it can lead to paradoxes like the famous Russell paradox. Consider the predicate $R(x) = x \notin x$, this predicate is true for x if x is not a member of itself and consider the class that contains all classes that has not them self as member. Does this class contain itself yes or no? If the class contain itself then by definition $R(x)$ should be true so the class should not contain itself leading to a contradiction. If the class does not contain itself then it satisfies $R(x)$, hence it is a member of itself again leading to a contradiction. So we can not test the predicate $R(x)$ for all classes and thus can not define the class of all classes for which $R(x)$ is true. The axiom of class construction allows us to create a new class in a safe way.

Axiom 1.9. (Axiom of Construction) *Let $P(x)$ be a statement about x [using mathematical logic] then there exists a class C such that $x \in C$ iff x is a element and $P(x)$ is true.*

***Notation* 1.10.** *This class C is noted as $C = \{x|P(x)\}$, note the use of lower cases for x, which is a visual indicator that x is a element.*

Note that that C consists of **elements** for which $P(x)$ is true, it is not enough that $P(x)$ is true to belong to C. A object must belong to a class [be a element or equivalently be a set] and $P(x)$ must be true to be a member of C. Let's see how that solves Russell's paradox. Define the class $R = \{x|x \notin x\}$ [Russel's class] and check if $R \in R$ or $R \notin R$ is true:

$\boldsymbol{R \in R}$. Then R is a element and $R \notin R$ giving the contradiction $R \in R \wedge R \notin R$

$\boldsymbol{R \notin R}$. Then R is not a element or $R \in R$ which as $R \notin R$ gives that R is not a element

So we have that R is not a element and indeed because of this that $R \notin R$. You can ask yourself if there actually exists elements, none of the axioms up to now can be used to get elements [or equivalent sets], for this we need extra axioms.

The axiom of construction can be used as a way of creating a sub-class of a given class.

Definition 1.11. *Let A be a class and $P(x)$ a predicate then $\{x \in A|P(x)\} = \{x|x \in A \wedge P(x)\}$*

Using the axiom of construction [axiom: 1.9] we can then define the universal class $\mathcal{U}$.

Definition 1.12. (Universal class) *The universal class $\mathcal{U}$ is defined by $\mathcal{U} = \{x|x = x\}$*

The universal class contains all the elements, as is expressed in the following theorem.

Theorem 1.13. *If x is a element then $x \in \mathcal{U}$*

Proof. Let x be a element then, as $x = x$ [see theorem: 1.8] we have that $x \in \mathcal{U}$ □

We use now the axiom of construction to define the union and intersection of two classes.

Definition 1.14. *Let A, B be two classes then the union of A and B, noted as $A \bigcup B$ is defined by*

$$A \bigcup B = \{x|x \in A \vee x \in B\}$$

Definition 1.15. *Let A, B be two classes then the union of A and B, noted as $A \bigcap B$ is defined by*

$$A \bigcap B = \{x|x \in A \wedge x \in B\}$$

Next we define the empty class, the class that does not contains a element.

Definition 1.16. *The empty class $\varnothing$ is defined by*

$$\varnothing = \{x|x \neq x\}$$

Theorem 1.17. *$\varnothing$ does not contains elements, meaning if x is a element then $x \notin \varnothing$*

Proof. We proof this by contradiction, so assume that there exists a element $x \in \varnothing$ then $x \neq x$, contradicting $x = x$ [see theorem: 1.8]. □

Theorem 1.18. *If A is a class then*

1. $\varnothing \subseteq A$
2. $A \subseteq \mathcal{U}$
3. *If* $A \subseteq \varnothing$ *then* $A = \varnothing$

Proof.

1. We proof this by contra-position, as $\varnothing \subseteq A$ is equivalent with $x \in \varnothing \Rightarrow x \in A$. We must proof that $x \notin A \Rightarrow x \notin \varnothing$. Well if $x \notin A$ then certainly $x \notin \varnothing$ [Theorem: 1.17] so that $x \notin A \Rightarrow x \notin \varnothing$.
2. If $x \in A$ then x is a element, hence $x \in \mathcal{U}$ by [Theorem: 1.13]
3. By (1) we have $\varnothing \subseteq A$ which together with $A \subseteq \varnothing$ proves by [theorem: 1.8] that $A = \varnothing$. □

We also have that every class with no elements is equal to the empty set [there is only one empty set]

Theorem 1.19. *If A is a a class such that $x \in A$ yields a contradiction then $A = \varnothing$*

Proof. Let $x \in A$ then we have a contradiction, so $x \in A$ must be false and thus $x \in A \Rightarrow x \in \varnothing$ is vacuously true which proves that $A \subseteq \varnothing$, combining this with [theorem: 1.18,1.8] proves that $A = \varnothing$ □

Corollary 1.20. *Let A be a class such that $A \neq \varnothing$ then $\exists x$ such that $x \in A$*

Proof. We proof this by contradiction. Assume that $\forall x$ we have $x \notin A$ then $x \in A$ yields the contradiction $x \in A \wedge x \notin A$, hence by [theorem: 1.19] $A = \varnothing$ which contradicts $A \neq \varnothing$. □

Definition 1.21. *Two classes A, B are disjoint iff $A \bigcap B = \varnothing$*

We define now the complement of a class

Definition 1.22. *Let A be a class then the complement of A noted by A^c is defined by*

$$A^c = \{x | x \notin A\}$$

Something similar to the complement of a class is the difference between two classes

Definition 1.23. *Let A, B be classes then the difference between A and B noted by $A \setminus B$ is defined by*

$$A \setminus B = \{x | x \in A \wedge x \notin B\} \underset{\text{shorter notation}}{=} \{x \in A | x \in B\}$$

We can express the difference of two classes using the intersection and the complement.

Theorem 1.24. *Let A, B be classes then*

$$A \setminus B = A \bigcap B^c$$

Proof. Let $x \in A \setminus B$ then $x \in A \wedge x \notin B$ so that $x \in A \wedge x \in B^c$, further if $x \in A \bigcap B^c$ then $x \in A \wedge x \notin B$. Using then the axiom of extent [axiom: 1.5]. □

1.2 Class operations

Theorem 1.25. *Let A, B are classes then we have*

1. $A \subseteq A \bigcup B$
2. $B \subseteq A \bigcup B$
3. $A \bigcap B \subseteq A$

4. $A\bigcap B\subseteq B$
5. $A\setminus B\subseteq A$
6. *If* C *is a class such that* $A\subseteq C$ *and* $B\subseteq C$ *then* $A\bigcup B\subseteq C$
7. *If* C *is a class such that* $A\subseteq C$ *and* D *a class such that* $B\subseteq D$ *then* $A\bigcup B\subseteq C\bigcup D$
8. *If* C *is a class such that* $C\subseteq A$ *and* $C\subseteq B$ *then* $C\subseteq A\bigcap B$
9. *If* C *is a class such that* $A\subseteq C$ *and* D *a class such that* $B\subseteq D$ *then* $A\bigcap B\subseteq C\bigcap D$

Proof.

1. If $x\in A$ then $x\in A\vee x\in B$ proving that $x\in A\bigcup B$, hence $A\subseteq A\bigcup B$
2. If $x\in B$ then $x\in A\vee x\in B$ proving that $x\in A\bigcup B$, hence $B\subseteq A\bigcup B$
3. If $x\in A\bigcap B$ then $x\in A\wedge x\in B$, hence $x\in A$ so that $x\in A$, hence $A\bigcap B\subseteq A$
4. If $x\in A\bigcap B$ then $x\in A\wedge x\in B$, hence $x\in B$ so that $x\in A$, hence $A\bigcap B\subseteq B$
5. If $x\in A\setminus B$ then $x\in A\wedge x\notin B$ so that $A\setminus B\subseteq A$
6. If $x\in A\bigcup B$ then $x\in A \underset{A\subseteq C}{\Rightarrow} x\in C$ or $x\in B \underset{B\subseteq C}{\Rightarrow} x\in C$ proving that $x\in C$
7. Using (1) $A\subseteq C\bigcup D$ and $B\subseteq C\bigcup D$, so using (6) we have $A\bigcup B\subseteq C\bigcup D$
8. If $x\in C$ then $x\in A$ and $x\in B$ so that $x\in A\bigcap B$
9. If $x\in A\bigcap B$ then $x\in A \underset{A\subseteq C}{\Rightarrow} x\in C$ and $x\in B \underset{B\subseteq D}{\Rightarrow} x\in D$ hence $x\in C\bigcap D$. □

Theorem 1.26. *If* A,B *are classes then we have*

1. $A\subseteq B$ *if and only if* $A\bigcup B=B$
2. $A\subseteq B$ *if and only if* $A\bigcap B=A$

Proof.

1.
   - **⇒.** If $x\in A\bigcup B\Rightarrow x\in A \underset{A\subseteq B}{\Rightarrow} x\in B$ and thus $A\bigcup B\subseteq B$. From the previous theorem [theorem: 1.25] we have $B\subseteq A\bigcup B$ so by 1.8 we have $A\bigcup B=B$
   - **⇐.** If $A\bigcup B=B$ then $x\in A\Rightarrow x\in A\bigcup B \underset{A\bigcup B=B}{\Rightarrow} x\in B$ and thus $A\subseteq B$
2.
   - **⇒.** If $x\in A \underset{A\subseteq B}{\Rightarrow} x\in B\Rightarrow x\in A\wedge x\in B\Rightarrow x\in A\bigcap B$ proving that $A\subseteq A\bigcap B$. From the previous theorem we have $A\bigcap B\subseteq A$ so by [theorem: 1.8] we have $A\bigcap B=A$
   - **⇐.** If $A\bigcap B=A$ we have $x\in A\Rightarrow x\in A\bigcap B\Rightarrow(x\in A\wedge x\in B)\Rightarrow x\in B$ so $A\subseteq B$. □

Theorem 1.27. (Absorption Laws) *If* A,B *are classes then*

1. $A\bigcup(A\bigcap B)=A$
2. $A\bigcap(A\bigcup B)=A$

Proof.

1. By [theorem: 1.25 we have $A\bigcap B\subseteq A$, hence using [theorem: 1.26] we have that $A\bigcup(A\bigcap B)=A$
2. By [theorem: 1.25] we have $A\subseteq A\bigcup B$, hence using [theorem: 1.26] we have that $A\bigcap(A\bigcup B)=A$ □

Theorem 1.28. *Let* A *be a class then* $(A^c)^c=A$

Proof. If $x\in(A^c)^c$ then x is a element and $x\notin A$ then $x\in A$ [for if $x\notin A$ we have $x\in A^c$]. If $x\in A$ then $x\notin A^c$ so that $x\in(A^c)^c$. □

Theorem 1.29. (DeMorgan's Law) *For all classes A, B, C we have*

1. $(A\bigcup B)^c = A^c\bigcap B^c$
2. $(A\bigcap B)^c = A^c\bigcup B^c$

Proof.

1. If $x \in (A\bigcup B)^c$ then $x \notin A\bigcup B$, so that $\neg(x \in A \vee x \in B) = x \notin A \wedge x \notin B$ proving that $x \in A^c\bigcap B^c$. If $x \in A^c\bigcap B^c$ then $x \notin A \wedge x \notin B = \neg(x \in A \vee x \in B)$, so that $x \notin A\bigcup B$ or $x \in (A\bigcup B)^c$. The proof follows then from the axiom of extent [axiom: 1.5]
2. If $x \in (A\bigcap B)^c$ then $x \notin A\bigcap B$, so that $\neg(x \in A \wedge x \in B) = x \notin A \vee x \notin B$ proving that $x \in A^c\bigcup B^c$. If $x \in A^c\bigcup B^c$ then $x \notin A \vee x \notin B = \neg(x \in A \wedge x \in B)$, so that $x \in (A\bigcap B)^c$. The proof follows then from axiom of extent [axiom: 1.5] □

Theorem 1.30. *Let A, B, C be classes then we have:*

commutativity.

1. $A\bigcup B = B\bigcup A$
2. $A\bigcap B = B\bigcap A$

idem potency.

1. $A\bigcup A = A$
2. $A\bigcap A = A$

associativity.

1. $A\bigcup (B\bigcup C) = (A\bigcup B)\bigcup C$
2. $A\bigcap (B\bigcap C) = (A\bigcap B)\bigcap C$

Distributivity.

1. $A\bigcup (B\bigcap C) = (A\bigcup B)\bigcap (A\bigcup C)$
2. $A\bigcap (B\bigcup C) = (A\bigcap B)\bigcup (A\bigcap C)$

Proof.

commutatitivity.

1. This follows from [axiom: 1.5] and
$$\begin{aligned} x \in A\bigcup B &\Leftrightarrow x \in A \vee x \in B \\ &\Leftrightarrow x \in B \vee x \in A \\ &\Leftrightarrow x \in B\bigcup A \end{aligned}$$
2. This follows from [axiom: 1.5] and
$$\begin{aligned} x \in A\bigcap B &\Leftrightarrow x \in A \wedge x \in B \\ &\Leftrightarrow x \in B \wedge x \in A \\ &\Leftrightarrow x \in B\bigcap A \end{aligned}$$

idem potency.

1. This follows from [axiom: 1.5] and
$$\begin{aligned} x \in A\bigcup A &\Leftrightarrow x \in A \vee x \in A \\ &\Leftrightarrow x \in A \end{aligned}$$
2. This follows from [axiom: 1.5] and
$$\begin{aligned} x \in A\bigcap A &\Leftrightarrow x \in A \wedge x \in A \\ &\Leftrightarrow x \in A \end{aligned}$$

associativity.

1. This follows from [axiom: 1.5] and

$$\begin{aligned} x \in A \bigcup (B \bigcup C) &\Leftrightarrow x \in A \vee x \in B \bigcup C \\ &\Leftrightarrow x \in A \vee (x \in B \vee x \in C) \\ &\Leftrightarrow (x \in A \vee x \in B) \vee x \in C \\ &\Leftrightarrow x \in A \bigcup B \vee x \in C \\ &\Leftrightarrow x \in \left(A \bigcup B\right) \bigcup C \end{aligned}$$

2. This follows from [axiom: 1.5] and

$$\begin{aligned} x \in A \bigcap (B \bigcap C) &\Leftrightarrow x \in A \vee x \in B \bigcap C \\ &\Leftrightarrow x \in A \wedge (x \in B \wedge x \in C) \\ &\Leftrightarrow (x \in A \wedge x \in B) \wedge x \in C \\ &\Leftrightarrow x \in A \bigcap B \wedge x \in C \\ &\Leftrightarrow x \in \left(A \bigcap B\right) \bigcap C \end{aligned}$$

Distributivity.

1. This follows from [axiom: 1.5] and

$$\begin{aligned} x \in A \bigcup (B \bigcap C) &\Leftrightarrow x \in A \vee x \in B \bigcap C \\ &\Leftrightarrow x \in A \vee (x \in B \wedge x \in C) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\ &\Leftrightarrow x \in A \bigcup B \wedge x \in A \bigcup C \\ &\Leftrightarrow x \in \left(A \bigcup B\right) \bigcap \left(A \bigcup C\right) \end{aligned}$$

2. This follows from [axiom: 1.5] and

$$\begin{aligned} x \in A \bigcap (B \bigcup C) &\Leftrightarrow x \in A \wedge x \in B \bigcup C \\ &\Leftrightarrow x \in A \wedge (x \in B \vee x \in C) \\ &\Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\ &\Leftrightarrow x \in A \bigcap B \wedge x \in A \bigcap C \\ &\Leftrightarrow x \in \left(A \bigcap B\right) \bigcup \left(A \bigcap C\right) \end{aligned}$$

$\square$

Theorem 1.31. *Let A, B, C be classes then we have*

1. $A \setminus (B \bigcup C) = (A \setminus B) \bigcap (A \setminus C)$
2. $A \setminus (B \bigcap C) = (A \setminus B) \bigcup (A \setminus C)$

Proof.

1.

$$\begin{aligned} A \setminus (B \bigcup C) &\underset{\text{theorem:1.24}}{=} A \bigcap (B \bigcup C)^c \\ &\underset{\text{theorem: 1.29}}{=} A \bigcap (B^c \bigcap C^c) \\ &\underset{\text{associativity}}{=} (A \bigcap B^c) \bigcap C^c \\ &\underset{\text{idem potency}}{=} ((A \bigcap A) \bigcap B^c) \bigcap C^c \\ &\underset{\text{associativity}}{=} (A \bigcap (A \bigcap B^c)) \bigcap C^c \\ &\underset{\text{commutativity}}{=} ((A \bigcap B^c) \bigcap A) \bigcap C^c \\ &\underset{\text{associativity}}{=} (A \bigcap B^c) \bigcap (A \bigcap C^c) \\ &\underset{\text{theorem:1.24}}{=} (A \setminus B) \bigcap (A \setminus C) \end{aligned}$$

2.

$$\begin{aligned} A\setminus(B\bigcap C) &\underset{\text{theorem:1.24}}{=} A\bigcap(B\bigcap C)^c \\ &\underset{\text{theorem: 1.29}}{=} A\bigcap(B^c\bigcup C^c) \\ &\underset{\text{Distributivity}}{=} (A\bigcap B^c)\bigcup(A\bigcap C^c) \\ &\underset{\text{theorem:1.24}}{=} (A\setminus B)\bigcup(A\setminus C) \end{aligned}$$

□

Theorem 1.32. *Let A be a class then we have:*

1. $\varnothing\bigcup A=A$
2. $\varnothing\bigcap\varnothing=\varnothing$
3. $A\bigcup\mathcal{U}=\mathcal{U}$
4. $A\bigcap\mathcal{U}=A$
5. $A\setminus A=\varnothing$

Proof.

1. As $\varnothing\subseteq A$ [theorem: 1.18] we have by [theorem: 1.26] that $\varnothing\bigcup A=A$
2. As $\varnothing\subseteq A$ [theorem: 1.18] we have by [theorem: 1.26] that $\varnothing\bigcap A=A$
3. As $A\subseteq\mathcal{U}$ [theorem 1.18] we have by [theorem: 1.26] that $A\bigcap\mathcal{U}=A$
4. As $A\subseteq\mathcal{U}$ [theorem 1.18] we have by [theorem: 1.26] that $A\bigcap\mathcal{U}=A$
5. Let $x\in A\setminus A$ then $x\in A\wedge x\notin A$ a contradiction, so by [theorem: 1.19] we have that $A\setminus A=\varnothing$ □

1.3 Cartesian products

If a is a element we can use the axiom of construction [axiom: 1.9] to define the class $\{x|x=a\}$, this leads to the following definition.

Definition 1.33. *If a is a element then $\{a\}=\{x|x=a\}$ is a class containing only one element. The class $\{a\}$ is called a **singleton**.*

Lemma 1.34. *If a,b are elements such that $a=b$ then $\{a\}=\{b\}$*

Proof. If $z\in\{a\}$ then $z=a$ which by $a=b$ and [theorem: 1.8] proves that $z=b$ hence $z\in\{b\}$. Likewise if $z\in\{b\}$ then $z=b$ which by $a=b$ and [theorem: 1.8] proves that $z=a$ hence $z\in\{a\}$. Using the axiom of extent [axiom: 1.5] it follows then that $\{a\}=\{b\}$ □

If a,b are elements then we can use the axiom of construction [axiom: 1.9] to define the class $\{x|x=a\vee x=b\}$ consisting of two elements. This leads to the following definition.

Definition 1.35. *If a,b are elements then $\{a,b\}=\{x|x=a\vee x=b\}$ is called a **unordered pair**.*

The next axiom ensures we can construct new elements from given elements.. It allows us to create classes that has as members pairs of elements.

Axiom 1.36. (Axiom of Pairing) *If a,b are elements then $\{a,b\}$ is a element*

Lemma 1.37. *If a is a element then $\{a,a\}=\{a\}$*

Proof.

$$\begin{aligned} x\in\{a,a\} &\Leftrightarrow x=a\vee x=a \\ &\Leftrightarrow x=a \\ &\Leftrightarrow x\in\{a\} \end{aligned}$$

□

Theorem 1.38. *If a is a element then $\{a\}$ is a element*

Proof. As a is a element we have by the axiom of pairing [axiom: 1.36] that $\{a, a\}$ is a element, which as $\{a\} \underset{\text{lemma: } 1.37}{=} \{a., a\}$ proves that $\{a\}$ is a element. □

The following lemma characterize equality of unordered pairs and will be used later to characterize equality of ordered pairs.

Lemma 1.39. *If x, y, x', y' are elements then*

$$\{x, y\} = \{x', y'\} \text{ implies } (x = x' \wedge y = y') \vee (x = y' \wedge y = x')$$

Proof. Lets's consider the following possible cases x, y:

$\boldsymbol{x = y}$**.** Then $\{x, y\} \underset{\text{lemma: } 1.37}{=} \{x\} = \{x', y'\}$. From $x' \in \{x', y'\} = \{x\}$ it follows that $x = x'$ and from $y' \in \{x', y'\} = \{x\}$ it follows that $y = x$. As $x = x'$ it follows from [theorem: 1.8] that $y = x'$. So we have that $(x = x' \wedge y = y')$ from which it follows that

$$(x = x' \wedge y = y') \vee (x = y' \wedge y = x')$$

$\boldsymbol{x \neq y}$**.** Then as $x \in \{x, y\} = \{x', y'\}$ we have by [axiom: 1.5] that $x \in \{x', y'\}$, so by definition we have for x either

$\boldsymbol{x = x'}$**.** Then as $y \in \{x, y\} = \{x', y'\}$ we have by [axiom: 1.5] that $y \in \{x', y'\}$, so by definition we have for y either:

$\boldsymbol{y = x'}$**.** As $x = x' \underset{\text{theorem: } 1.8}{\Rightarrow} x = y$ we contradict $x \neq y$ so this case does not apply

$\boldsymbol{y = y'}$**.** Then $(x = x' \wedge y = y')$ hence $(x = x' \wedge y = y') \vee (x = y' \wedge y = x')$

$\boldsymbol{x = y'}$**.** Then as $y \in \{x, y\} = \{x', y'\}$ we have by [axiom: 1.5] that $y \in \{x', y'\}$, so by definition we have for y either:

$\boldsymbol{y = x'}$**.** Then $(x = y' \wedge y = x')$ hence $(x = x' \wedge y = y') \vee (x = y' \wedge y = x')$

$\boldsymbol{y = y'}$**.** As $x = y' \underset{\text{theorem: } 1.8}{\Rightarrow} x = y$ we contradict $x \neq y$ so this case does not apply

So in all cases that apply we have

$$(x = x' \wedge y = y') \vee (x = y' \wedge y = x')$$ □

Lemma 1.40. *If x, y, x', y' are elements such that $(x = x' \wedge y = y') \vee (x = y' \wedge y = x')$ then $\{x, y\} = \{x, y'\}$*

Proof. Let $z \in \{x, y\}$ then either:

$\boldsymbol{z = x}$**.** then if $x = x' \wedge y = y'$ we have using [theorem: 1.8] that $z = x'$, hence by definition $z \in \{x', y'\}$ and if $x = y' \wedge y = x'$ we have using [theorem: 1.8] that $z = y'$, hence by definition $x \in \{x', y'\}$

$\boldsymbol{z = y}$**.** then if $x = x' \wedge y = y'$ we have using [theorem: 1.8] that $z = y'$, hence by definition $z \in \{x', y'\}$ and if $x = y' \wedge y = x'$ we have using [theorem: 1.8] that $z = x'$, hence by definition $x \in \{x', y'\}$

which proves that

$$\{x, y\} \subseteq \{x', y'\} \tag{1.5}$$

Let $z \in \{x', y'\}$ then either:

$\boldsymbol{z = x'}$**.** then if $x = x' \wedge y = y'$ we have using [theorem: 1.8] that $z = x$, hence by definition $z \in \{x, y\}$ and if $x = y' \wedge y = x'$ we have using [theorem: 1.8] that $z = y$, hence by definition $x \in \{x, y\}$

$\boldsymbol{z = y}$**.** then if $x = x' \wedge y = y'$ we have using [theorem: 1.8] that $z = y$, hence by definition $z \in \{x, y\}$ and if $x = y' \wedge y = x'$ we have using [theorem: 1.8] that $z = x$, hence by definition $x \in \{x, y\}$

which proves that

$$\{x', y'\} \subseteq \{x, y\} \tag{1.6}$$

Using [theorem: 1.8] on [eq: 1.5,1.6] proves that

$$\{x = y\} = \{x' = y'\}$$ □

The above lemma actually shows that the order of the elements in unordered pairs do not matter, to remedy this we construct a ordered pair.

Definition 1.41. *If a, b are elements then*

$$(a, b) = \{\{a\}, \{a, b\}\}$$

***Note* 1.42.** *As $\{a\}, \{a, b\}$ are elements we have again that $\{\{a\}, \{a, b\}\}$ is a element, hence (a, b) is also a element.*

Next we show that the order of elements is important for a tuple

Theorem 1.43. *Let x, y, x', y' are elements then*

$$(x, y) = (x', y') \Leftrightarrow x = x' \wedge y = y'$$

Proof.

⇒. If $(x, y) = (x', y')$ then by definition

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$$

By [lemma: 1.39] we have either:

$\boldsymbol{\{x\} = \{x'\} \wedge \{x, y\} = \{x', y'\}}$**.** then, as $x \in \{x\}$, we have by definition $x = x'$, using [lemma: 1.39] again we have either:

$\boldsymbol{x = x' \wedge y = y'}$**.** Then $x = x' \wedge y = y'$

$\boldsymbol{x = y' \wedge y = x'}$**.** Then by [theorem: 1.8] and $x = x'$ we have $y' = x'$ so that by [theorem: 1.8] again $y = y'$. Hence we have $x = x' \wedge y = y'$

$\boldsymbol{\{x\} = \{x', y'\} \wedge \{x, y\} = \{x'\}}$**.** Then as $x', y' \in \{x', y'\} = \{x\}$ we have $x' = x \wedge y' = x$, as $x, y \in \{x, y\} = \{x'\}$ we have $x = x' \wedge y = x'$. Using [theorem: 1.8] on $y' = x \wedge x = x' \wedge y = x'$ we have $y = y'$. Hence $x = x' \wedge y = y'$.

So in all cases we have

$$x = x' \wedge y = y'$$

⇐. As $x = x'$ it follows from [lemma: 1.34] that $\{x\} = \{x'\}$, from $x = x' \wedge y = y'$ we have by [lemma: 1.40] that $\{x, y\} = \{x', y'\}$. Using [lemma: 1.40] gives then that $\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\}$ which by definition gives

$$(x, y) = (x', y')$$ □

We are now ready to define the Cartesian product of two classes, using the axiom of construction [axiom: 1.9].

Definition 1.44. *If A, B are classes then the **Cartesian product** of A and B noted by $A \times B$ is defined as*

$$A \times B = \{z | z = (a, b) \wedge a \in A \wedge b \in B\}$$

***Notation* 1.45.** *Instead of writing $\{z | z = (a, b) \wedge a \in A \wedge b \in A\}$ we use in the future the shorter notation $\{(a, b) | a \in A \wedge b \in B\}$*

A special case of the Cartesian product is the Cartesian product of empty sets.

Example 1.46. $\varnothing = \varnothing \times \varnothing$

Proof. If $z \in \varnothing \times \varnothing$ then there exists a $x, y \in \varnothing$ such that $z = (x, y)$ which contradict $x, y \notin \varnothing$ [theorem: 1.17] hence by 1.19 we have $\varnothing \times \varnothing = \varnothing$. □

Theorem 1.47. *Let A be a class then $A \times \varnothing = \varnothing$ and $\varnothing \times A = \varnothing$*

Proof. If $z \in A \times \varnothing$ then $z = (x, y)$ where $y \in \varnothing$, which contradicts $y \notin \varnothing$ [theorem: 1.17], so using [theorem: 1.19] we have that

$$A \times \varnothing = \varnothing$$

Likewise if $x \in \varnothing \times A$ then $z = (x, y)$ where $x \in \varnothing$, which contradicts $x \notin \varnothing$ [theorem: 1.17], so using [theorem: 1.19] we have that

$$\varnothing \times A = \varnothing$$

□

Theorem 1.48. *If A, B, C, D are classes then we have:*

1. *If $A \subseteq B \wedge C \subseteq D$ then $A \times C \subseteq B \times D$*
2. *Let $A \neq \varnothing \wedge C \neq \varnothing$ then if $A \times C \subseteq B \times D$ it follows that $A \subseteq B \wedge C \subseteq D$*
3. *Let $A \neq \varnothing \wedge B \neq \varnothing \wedge C \neq \varnothing$ then $A \times C = B \times D \Leftrightarrow A = B \wedge C = D$*

Proof.

1. Let $z \in A \times C$ then there exists a $x \in A$ and $y \in C$ such that $z = (x, y)$. As $A \subseteq B \wedge C \subseteq D$ it follows that $x \in B \wedge y \in D$ so that $z = (x, y) \in B \times D/$ Hence

$$A \times C \subseteq B \times D$$

2. Let $x \in A$ then, as $C \neq \varnothing$, we have by [corollary: 1.20] the existence of a $y \in C$, then $(x, y) \in A \times C$ which as $A \times C \subseteq B \times D$ proves that $(x, y) \in B \times D$. By definition we have then that $x \in B$ proving

$$A \subseteq B$$

Likewise, let $y \in C$ then, as $A \neq \varnothing$ we have by [corollary: 1.20] the existence of a $x \in A$, hence $(x, y) \in A \times C$, which as $A \times C \subseteq B \times D$, proves $(x, y) \in B \times D$ and by definition $y \in D$. Hence

$$C \subseteq D$$

3.

⇒. First as $A \times C = B \times D$ we have by [theorem: 1.8] that $A \times C \subseteq B \times D$, using (2) proves then that

$$A \subseteq B \wedge C \subseteq B \tag{1.7}$$

Next as $A \times C = B \times D$ we have by [theorem: 1.8] that $B \times D \subseteq A \times C$, using (2) proves then that

$$B \subseteq A \wedge C \subseteq D \tag{1.8}$$

Combining then [eq 1.7,1.8] with [theorem: 1.8] proves

$$A = B \wedge C = D$$

⇐. As $A = B \wedge C = D$ we have by [theorem: 1.8] that $A \subseteq B$, $C \subseteq D$, $B \subseteq A$,$D \subseteq C$ which using (1) gives that $A \times C \subseteq B \times D \wedge B \times D \subseteq A \times C$. Using [theorem: 1.8 it follows then that

$$A \times C = B \times D$$

□

Theorem 1.49. *Let A,B,C and D be classes then we have*

1. *$A \times (B \bigcap C) = (A \times B) \bigcap (A \times C)$*

2. $A \times (B \bigcup C) = (A \times B) \bigcup (A \times C)$
3. $(A \times B) \bigcap (C \times D) = (A \bigcap C) \times (B \bigcap D)$
4. $(B \bigcap C) \times A = (B \times A) \bigcap (C \times A)$
5. $(B \bigcup C) \times A = (B \times A) \bigcup (C \times A)$
6. $(A \times B) \setminus (C \times D) = ((A \setminus C) \times B) \bigcup (A \times (B \setminus D))$
7. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$
8. $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

Proof.

1. We have

$$\begin{aligned} z \in A \times \left(B \bigcap C\right) &\Leftrightarrow z = (x,y) \wedge x \in A \wedge y \in \left(B \bigcap C\right) \\ &\Leftrightarrow z = (x,y) \wedge x \in A \wedge (y \in B \wedge y \in C) \\ &\Leftrightarrow (z = (x,y) \wedge x \in A \wedge y \in B) \wedge (z = (x,y) \wedge x \in A \wedge y \in C) \\ &\Leftrightarrow z \in A \times B \wedge z \in A \times C \\ &\Leftrightarrow z \in (A \times B) \bigcap (A \times C) \end{aligned}$$

2. We have

$$\begin{aligned} z \in A \times \left(B \bigcup C\right) &\Leftrightarrow z = (x,y) \wedge x \in A \wedge y \in \left(B \bigcup C\right) \\ &\Leftrightarrow z = (x,y) \wedge x \in A \wedge (y \in B \vee y \in C) \\ &\Leftrightarrow (z = (x,y) \wedge x \in A \wedge y \in B) \vee (z = (x,y) \wedge x \in A \wedge y \in C) \\ &\Leftrightarrow z \in A \times B \vee z \in A \times C \\ &\Leftrightarrow z \in (A \times B) \bigcup (A \times C) \end{aligned}$$

3. We have

$$\begin{aligned} z \in (A \times B) \bigcap (C \times D) &\Leftrightarrow z \in A \times B \wedge z \in C \times D \\ &\Leftrightarrow (z = (x,y) \wedge x \in A \wedge y \in B) \wedge (z = (x',y') \wedge \\ &\qquad x' \in C \wedge y' \in D) \\ &\underset{(x,y)=z=(x',y') \Rightarrow x=x', y=y'}{\Leftrightarrow} z = (x,y) \wedge x \in A \wedge y \in B \wedge x \in C \wedge y \in D \\ &\Leftrightarrow z = (x,y) \wedge (x \in A \wedge x \in C) \wedge (y \in B \wedge \\ &\qquad y \in D) \\ &\Leftrightarrow z = (x,y) \wedge \left(x \in A \bigcap C\right) \wedge \left(y \in B \bigcap D\right) \\ &\Leftrightarrow z \in \left(A \bigcap C\right) \times \left(B \bigcap D\right) \end{aligned}$$

4. We have

$$\begin{aligned} z \in \left(B \bigcap C\right) \times A &\Leftrightarrow z = (x,y) \wedge x \in B \bigcap C \wedge y \in A \\ &\Leftrightarrow z = (x,y) \wedge x \in B \wedge x \in C \wedge y \in A \\ &\Leftrightarrow (z = (x,y) \wedge x \in B \wedge y \in A) \wedge (z = (x,y) \wedge x \in C \wedge y \in A) \\ &\Leftrightarrow z \in B \times A \wedge z \in C \times A \\ &\Leftrightarrow z \in (B \times A) \bigcap (C \times A) \end{aligned}$$

5. We have

$$\begin{aligned} z \in \left(B \bigcup C\right) \times A &\Leftrightarrow z = (x,y) \wedge x \in B \bigcup C \wedge y \in A \\ &\Leftrightarrow z = (x,y) \wedge (x \in B \vee x \in C) \wedge y \in A \\ &\Leftrightarrow (z = (x,y) \wedge x \in B \wedge y \in A) \vee (z = (x,y) \wedge x \in C \wedge y \in A) \\ &\Leftrightarrow (z \in B \times A) \vee (z \in C \times A) \\ &\Leftrightarrow z \in (B \times A) \bigcup (C \times A) \end{aligned}$$

6. We have

$$\begin{aligned}
z \in (A \times B) \setminus (C \times D) & \Leftrightarrow \\
(z = (x, y) \wedge x \in A \wedge y \in B) \wedge (x, y) \notin C \times D & \Leftrightarrow \\
(z = (x, y) \wedge x \in A \wedge y \in B) \wedge \neg(x \in C \wedge y \in D) & \Leftrightarrow \\
(z = (x, y) \wedge x \in A \wedge y \in B) \wedge (x \notin C \vee y \notin D) & \Leftrightarrow \\
(z = (x, y) \wedge x \in A \wedge y \in B \wedge x \notin C) \vee (z = (x, y) \wedge x \in A \wedge y \in B \wedge y \notin D) & \Leftrightarrow \\
z = (x, y) \wedge [(x, y) \in (A \setminus C) \times B \vee (x, y) \in A \times (B \setminus D)] & \Leftrightarrow \\
z \in ((A \setminus C) \times B) \bigcup (A \times (B \setminus D)) & \Leftrightarrow
\end{aligned}$$

7. We have

$$\begin{aligned}
(A \times C) \setminus (B \times C) & \underset{(6)}{=} ((A \setminus C) \times B) \bigcup (A \times (C \setminus C)) \\
& \underset{[\text{theorem: } 1.32]}{=} ((A \setminus C) \times B) \bigcup (A \times \varnothing) \\
& \underset{[\text{theorem: } 1.47}{=} ((A \setminus C) \times B) \bigcup \varnothing \\
& \underset{[\text{theorem: } 1.32]}{=} (A \setminus C) \times B
\end{aligned}$$

8. We have

$$\begin{aligned}
(A \times B) \setminus (A \times C) & \underset{(6)}{=} ((A \setminus A) \times B) \bigcup (A \times (B \setminus C)) \\
& \underset{[\text{theorem: } 1.32]}{=} (\varnothing \times B) \bigcup (A \times (B \setminus C)) \\
& \underset{[\text{theorem: } 1.47}{=} \varnothing \bigcup (A \times (B \setminus C)) \\
& \underset{[\text{theorem: } 1.32]}{=} A \times (B \setminus C)
\end{aligned}$$

□

1.4 Sets

Remember that that another name for **element** is **set** [definition: 1.2]. Up to now we have used the name **element**, because we want to think of a element as a member of a class. However a element is also a class and can contain other elements. If we want to stress the collection aspect then we use the word **set** instead of **element**. The convention is to use uppercase to represent a set and lower cases for a element. Of course set and element are the same thing, we just want to stress different aspects of the same thing. Note that we have two kinds of classes classes that are a member of another class and classes that are not a member of a class. This leads to the following definition.

Definition 1.50. *A class A is a* ***set*** *[or* ***element****] if there exists a class B such that $A \in B$. A class that is never a member of another class is called a* ***proper class****.*

Up to know we had axioms that given a element/set create a new element/set, but we have not ensured the existence of a element/set. To this we must first define the concept of a successor set.

Definition 1.51. *A set S is a* ***successor set*** *iff*

1. $\varnothing \in S$
2. *If $X \in S$ then $X \bigcup \{X\} \in S$*

Of course nothing proves that successor set's exists, to ensure the existence of a successor set we have the axiom of infinity.

Axiom 1.52. (Axiom of Infinity) *There exists a* ***successor set***

This axiom ensures that we have at least one set. We can then use the other axioms about elements/sets to create new elements. Later we will use the Axiom of Infinity to create the Natural Numbers, form which we build all the other numbers (integers, rationals, reals, complex numbers). The Axiom of Infinity ensures also that the empty class is actually a set.

Theorem 1.53. *$\varnothing$ is a set*

Proof. The Axiom of Infinity [axiom: 1.52] ensures the existence of a successor set S. By definition we have then that $\varnothing \in S$ which proves that $\varnothing$ is a set. □

So now we have two sets to start with, the successor set and the empty set. We can use the Axiom of Pairing [axiom: 1.36] to create new sets like singletons, unordered pairs and pairs. We introduce now extra axioms to create new sets given existing sets.

Axiom 1.54. (Axiom of Subsets) *Every sub-class of a set is a set*

As a application we proof that the intersection of two sets is a set

Theorem 1.55. *Let A, B be sets then $A \bigcap B$ is a set*

Proof. By [theorem: 1.25] we have that $A \bigcap B \subseteq A$, so by the axiom of infinity [axiom: 1.52] it follows that $A \bigcap B$ is a set. □

We define now a more general concept of union and intersection

Definition 1.56. *Let $\mathcal{A}$ be a class then using the Axiom of Construction [axiom: 1.9] we define $\bigcup \mathcal{A} = \{x \mid \exists y \in \mathcal{A}$ such that $x \in y\}$*

Definition 1.57. *Let $\mathcal{A}$ be a class then using the Axiom of Construction [axiom: 1.9] we define $\bigcap \mathcal{A} = \{x \mid \forall y \in \mathcal{A}$ we have $x \in y\}$*

Example 1.58. Let A be a class then

1. $\bigcup \{A\} = A$
2. $\bigcap \{A\} = A$
3. $\bigcup \varnothing = \varnothing$

Proof.

1. $$\begin{aligned} x \in \bigcup \{A\} &\Leftrightarrow \exists y \in \{A\} \text{ with } x \in y \\ &\underset{y \in \{A\} \Leftrightarrow y = A}{\Leftrightarrow} x \in A \end{aligned}$$

   proving that
   $$\bigcup \{A\} = A$$

2. $$\begin{aligned} x \in \bigcap \{A\} &\Leftrightarrow \forall y \in \{A\} \text{ we have } x \in y \\ &\underset{y \in \{A\} \Leftrightarrow y = A}{\Leftrightarrow} x \in A \end{aligned}$$

   proving that
   $$\bigcap \{A\} = A$$

3. Assume that $x \in \varnothing$ then $\exists y \in \varnothing$ such that $x \in y$ which lead by the definition of $\varnothing$ [definition: 1.16] to the contradiction that $y \neq y$. □

Example 1.59. Let A and B classes then

1. $\bigcup \{A, B\} = A \bigcup B$

2. $\bigcap \{A, B\} = A \bigcap B$

Proof.

1.
$$\begin{aligned} x \in \bigcup \{A, B\} &\Leftrightarrow \exists y \in \{A, B\} \text{ with } x \in y \\ &\underset{y \in \{A,B\} \Leftrightarrow y = A \vee y = B}{\Leftrightarrow} x \in A \vee x \in B \\ &\Leftrightarrow x \in A \bigcup B \end{aligned}$$

proving that

$$\bigcup \{A, B\} = A \bigcup B$$

2.
$$\begin{aligned} x \in \bigcap \{A, B\} &\Leftrightarrow \forall y \in \{A, B\} \text{ with } x \in y \\ &\underset{y \in \{A,B\} \Leftrightarrow y = A \vee y = B}{\Leftrightarrow} x \in A \wedge x \in B \\ &\Leftrightarrow x \in A \bigcap B \end{aligned}$$

proving that

$$\bigcap \{A, B\} = A \bigcap B$$

□

Theorem 1.60. *If $\mathcal{A}$ is a class*

1. *If $A \in \mathcal{A}$ then $\bigcap \mathcal{A} \subseteq A$*
2. *If $A \in \mathcal{A}$ then $A \subseteq \bigcup \mathcal{A}$*
3. *If $\forall A \in \mathcal{A}$ we have $C \subseteq A$ then $C \subseteq \bigcap \mathcal{A}$*
4. *If $\forall A \in \mathcal{A}$ we have $A \subseteq C$ then $\bigcup \mathcal{A} \subseteq C$*
5. *If $\mathcal{A} \neq \varnothing$ then $\bigcap \mathcal{A}$ is a set*

Proof.

1. Let $A \in \mathcal{A}$ then if $x \in \bigcap \mathcal{A}$ we have by definition of $\bigcap \mathcal{A}$ that $x \in A$. Hence $\bigcap \mathcal{A} \subseteq A$
2. If $x \in A$ then $\exists y \in \mathcal{A}$ such that $x \in y$ [take $y = A$] so that $x \in \bigcup \mathcal{A}$
3. If $x \in C$ then $\forall A \in \mathcal{A}$ we have as $C \in A$ that $x \in A$ so that $x \in \bigcap \mathcal{A}$
4. If $x \in \bigcup \mathcal{A}$ then $\exists A \in \mathcal{A}$ such that $x \in A$ which as $A \subseteq C$ proves that $x \in A$
5. As $\mathcal{A} \neq \varnothing$ there exists a $A \in \mathcal{A}$, which by definition means that A is a set. Using (1) we have $\bigcap \mathcal{A} \subseteq A$, applying then the Axiom of Subsets [axiom: 1.54] it follows that $\bigcap \mathcal{A}$ is a set. □

The above is not applicable for unions, however we state the Axiom of Unions that will ensure that $\bigcup \mathcal{A}$ is a set if $\mathcal{A}$ is a set

Axiom 1.61. (Axiom of Unions) *If $\mathcal{A}$ is a set then $\bigcup \mathcal{A}$ is a set*

A consequence of the above axiom is that the union of two sets is a set

Theorem 1.62. *Let A, B be tow sets then $A \bigcup B$ is a set*

Proof. Using the Axiom of Pairing [axiom: 1.36] we have that $\{A, B\}$ is a set. Further

$$\begin{aligned} x \in A \bigcup B &\Leftrightarrow x \in A \vee x \in B \\ &\Leftrightarrow \exists C \in \{A, B\} \text{ with } x \in C \\ &\Leftrightarrow \bigcup \{A, B\} \end{aligned}$$

proving by the Axiom of Union [axiom: 1.61] we have that $A \bigcup B$ is a set. □

Definition 1.63. *Let A be a set then we use the Axiom of Construction to define $\mathcal{P}(A)$ by*

$$\mathcal{P}(A)=\{B|B\subseteq A\}$$

We introduce now the Axiom of Power Sets to ensure that $\mathcal{P}(A)$ is a set, called the **power set** of A.

Axiom 1.64. (Axiom of Power Sets) *If A is a set then $\mathcal{P}(A)$ is a set*

Theorem 1.65. *If A is a set and $P(X)$ a predicate then $\{X|X\subseteq A\wedge P(X)\}$ is a set.*

Proof. If $B\in\{X|X\subseteq A\wedge P(X)\}$ then $B\subseteq A$ so that $B\in\mathcal{P}(A)$, proving that

$$\{X|X\subseteq A\wedge P(X)\}\subseteq\mathcal{P}(A)$$

Using the Axiom of Power Sets [axiom: 1.64] $\mathcal{P}(A)$ is a set, so we can use the Axiom of Subsets to prove that $\{X|X\subseteq A\wedge P(X)\}$ is a set. □

Lemma 1.66. *If A,B are classes then $A\times B\subseteq\mathcal{P}(\mathcal{P}(A\bigcup B))$*

Proof. Let $z\in A\times B$ then there exists a $x\in A$ and a $y\in B$ so that $z=(x,y)$. Now if $e\in\{x\}$ then $e=x$ proving that $e\in A$, hence we have, by definition of the union, that $\{x\}\subseteq A\bigcup B$. By definition of the $\mathcal{P}(A\bigcup B)$ set it follows then that

$$\{x\}\in\mathcal{P}\left(A\bigcup B\right)$$

Likewise if $e\in\{x,y\}$ then either $e=x\Rightarrow e\in A$ or $e=y\Rightarrow e\in B$, hence ,by definition of the union, we have $\{x,y\}\subseteq A\bigcup B$. Using the definition $\mathcal{P}(A\bigcup B)$ we have then

$$\{x,y\}\in\mathcal{P}\left(A\bigcup B\right)$$

Now if $e\in\{\{x\},\{x,y\}\}$ then either $e=\{x\}\in\mathcal{P}(A\bigcup B)$ or $e=\{z,y\}\in\mathcal{P}(A\bigcup B)$ which proves that $\{\{x\},\{x,y\}\}\subseteq\mathcal{P}(A\bigcup B)$ or

$$z\in\{\{x\},\{x,y\}\}\in\mathcal{P}\left(\mathcal{P}\left(A\bigcup B\right)\right)$$

giving finally

$$A\times B\subseteq\mathcal{P}\left(\mathcal{P}\left(A\bigcup B\right)\right)$$ □

Theorem 1.67. *If A and B are sets then $A\times B$ is a set*

Proof. As A,B are sets we have by [theorem: 1.62] that $A\bigcup B$ is a set, using the Axiom of Power sets [axiom: 1.64] it follows that $\mathcal{P}(A\bigcup B)$ is a set, using the Axiom of Power sets [axiom: 1.64] again proves that $\mathcal{P}(\mathcal{P}(A\bigcup B))$ is a set. Finally by [lemma: 1.66] we have that $A\times B\subseteq\mathcal{P}(\mathcal{P}(A\bigcup B))$, which using the Axiom of Subsets [axiom: 1.54] proves that

$$A\times B \text{ is a set}$$ □

Chapter 2
Partial Functions and Functions

2.1 Pairs and Triples

Although we have already defined the concept of a pair, we can not simple extend this to pairs (and later triples) of classes. If A, B are pure classes (classes that are not elements) then we can not just form $(A, B) = \{A, \{B\}\}$ because this would mean that A, B are elements and not pure classes. So we need another way of forming pairs, triples and so on.

Definition 2.1. *If A, B are classes then $\langle A, B\rangle$ is defined by $\langle A, B\rangle = (A \times \{\varnothing\})\bigcup (B \times \{\{\varnothing\}\})$*

We show now that from $\langle A, B\rangle = \langle A',' B\rangle$ it follows that $A = A' \wedge B = B'$, first we need some lemma's

Lemma 2.2. *We have $\varnothing \neq \{\varnothing\}$*

Proof. Assume that $\{\varnothing\} = \varnothing$ then, as $\varnothing \in \{\varnothing\}$ it follows that $\varnothing$ which is a contradiction, hence

$$\varnothing \neq \{\varnothing\}$$

□

Lemma 2.3. *If A, B, C, D are classes then $\langle A, B\rangle = \langle C, D\rangle \Leftrightarrow A = C \wedge B = D$*

Proof.

⇒. Assume that $\langle A, B\rangle = \langle C, D\rangle$ then by definition

$$(A \times\{\varnothing\})\bigcup (B \times \{\{\varnothing\}\}) = (C \times \{\varnothing\})\bigcup (D \times \{\{\varnothing\}\}) \tag{2.1}$$

Let now $x \in A$ then $(x, \varnothing) \in (A \times \{\varnothing\})$ so that by the axiom of extent [axiom: 1.5] and [eq: 2.1]

$$(x, \varnothing) \in (C \times \{\varnothing\})\bigcup (D \times \{\{\varnothing\}\})$$

which by the definition of the union gives

$$(x, \varnothing) \in C \times \{\varnothing\} \vee (x, \varnothing) \in D \times \{\{\varnothing\}\} \tag{2.2}$$

Now if $(x, \varnothing) \in D \times \{\{\varnothing\}\}$ then $\varnothing \in \{\{\varnothing\}\}$ or $\varnothing = \{\varnothing\}$ which is impossible by [lemma: 2.2] so that by [eq: 2.2] we have $(x, \varnothing) \in C \times \{\varnothing\}$, hence $x \in C$. This proves that

$$A \subseteq C \tag{2.3}$$

Likewise, let $x \in C$ then $(x, \varnothing) \in (C \times \{\varnothing\})$ so that by the axiom of extent [axiom: 1.5] and [eq: 2.1

$$(x, \varnothing) \in (A \times \{\varnothing\})\bigcup (B \times \{\{\varnothing\}\})$$

which by the definition of the union gives

$$(x, \varnothing) \in A \times \{\varnothing\} \vee (x, \varnothing) \in B \times \{\{\varnothing\}\} \tag{2.4}$$

Now if $(x, \varnothing) \in B \times \{\{\varnothing\}\}$ then $\varnothing \in \{\{\varnothing\}\}$ or $\varnothing = \{\varnothing\}$ which is impossible by [lemma: 2.2] so that by [eq: 2.4] we have $(x, \varnothing) \in C \times \{\varnothing\}$, hence $x \in A$. This proves that

$$C \subseteq A \tag{2.5}$$

Combining [eq: 2.3,2.5] with [theorem: 1.8] proves

$$A = C$$

Further if $x \in B$ then $(x, \{\varnothing\}) \in B \times \{\{\varnothing\}\}$ so that by the axiom of extent [axiom: 1.5] and [eq: 2.1]

$$(x, \{\varnothing\}) \in (C \times \{\varnothing\}) \bigcup (D \times \{\{\varnothing\}\})$$

or using the definition of the union that

$$(x, \{\varnothing\}) \in C \times \{\varnothing\} \vee (x, \{\varnothing\}) \in D \times \{\{\varnothing\}\} \tag{2.6}$$

If $(x, \{\varnothing\}) \in C \times \{\varnothing\}$ then $\{\varnothing\} \in \{\varnothing\}$ or $\{\varnothing\} = \varnothing$ which is impossible by [lemma: 2.2], so by [eq: 2.6] we have that $(x, \{\varnothing\}) \in D \times \{\{\varnothing\}\}$, hence $x \in D$. This proves that

$$B \subseteq D \tag{2.7}$$

Likewise, if $x \in D$ then $(x, \{\varnothing\}) \in D \times \{\{\varnothing\}\}$ so that by the axiom of extent [axiom: 1.5] and [eq: 2.1]

$$(x, \{\varnothing\}) \in (A \times \{\varnothing\}) \bigcup (B \times \{\{\varnothing\}\})$$

or using the definition of the union that

$$(x, \{\varnothing\}) \in A \times \{\varnothing\} \vee (x, \{\varnothing\}) \in B \times \{\{\varnothing\}\} \tag{2.8}$$

If $(x, \{\varnothing\}) \in A \times \{\varnothing\}$ then $\{\varnothing\} \in \{\varnothing\}$ or $\{\varnothing\} = \varnothing$ which is impossible by [lemma: 2.2], so by [eq: 2.8] we have that $(x, \{\varnothing\}) \in B \times \{\{\varnothing\}\}$, hence $x \in B$. This proves that

$$D \subseteq B \tag{2.9}$$

Combining [eq: 2.7,2.9] with [theorem: 1.8] proves

$$B = D$$

⇐. Assume that $A = C \wedge B = D$ then

$$\begin{aligned}
x \in \langle A, B \rangle &\Leftrightarrow x \in (A \times \{\varnothing\}) \bigcup (B \times \{\{\varnothing\}\}) \\
&\Leftrightarrow x \in A \times \{\varnothing\} \vee x \in B \times \{\{\varnothing\}\} \\
&\Leftrightarrow (x = (a, \varnothing) \wedge a \in A) \vee (x = (b, \{\varnothing\}) \wedge b \in B) \\
&\underset{[\text{axiom: } 1.5]}{\Leftrightarrow} (x = (a, \varnothing) \wedge a \in C) \vee (x = (b, \{\varnothing\}) \wedge b \in D) \\
&\Leftrightarrow x \in (C \times \{\varnothing\}) \bigcup (D \times \{\{\varnothing\}\}) \\
&\Leftrightarrow e \in \langle C, D \rangle
\end{aligned}$$

so that by the Axiom of Extent [axiom: 1.5]

$$\langle A, B \rangle = \langle C, D \rangle$$

□

We can now easily extend $\langle A, B \rangle$ to a triple $\langle A, B, C \rangle$.

Definition 2.4. *Let A, B, C be classes then $\langle A, B, C \rangle$ is defined by*

$$\langle A, B, C \rangle = \langle \langle A, B \rangle, C \rangle$$

Lemma 2.5. *Let A, B, C, D, E, F be classes then*

$$\langle A, B, C \rangle = \langle D, E, F \rangle \Leftrightarrow A = D \wedge B = E \wedge C = F$$

Proof.

⇒. Assume that $\langle A, B, C \rangle = \langle D, E, F \rangle$ then by definition $\langle \langle A, B \rangle, C \rangle = \langle \langle D, E \rangle, F \rangle$, by [lemma: 2.3] then $C = F \wedge \langle A, B \rangle = \langle D, E \rangle$, using [lemma: 2.3] again proves then $A = D \wedge B = E$.

$\Leftarrow$. Assume that $A = D \wedge B = E \wedge C = F$ then by [lemma: 2.3] $\langle A, B\rangle = \langle D, E\rangle$, using [lemma: 2.3] again we have $\langle\langle A, B\rangle, C\rangle = \langle\langle D, E\rangle, F\rangle$ which by definition proves that

$$\langle A, B, C\rangle = \langle D, E, F\rangle$$

□

2.2 Partial functions and Functions

The concept of a function as a mapping of one value to a unique value is used throughout mathematics, especially in analysis, which is essential a theory of functions. Note that a function maps a value x to a **unique** value y which in the context of a set theory defines a pair (x, y). This leads to the following definition of a graph.

2.2.1 Partial function

Definition 2.6. *Then a triple $\langle A, B, f\rangle$ is a **partial function between A and B** if*

1. $f \subseteq A \times B$
2. *If* $(x, y) \in f \wedge (x, y') \in f$ *then* $y = y'$

*we class f the **graph** of the function.*

Remark 2.7. Instead of writing $\langle A, B, f\rangle$ for a partial function between A and B we use the notation $f: A \rightarrow B$ or $A \xrightarrow{f}$ B. Further the condition (2) ensures that only one value can be associated with x. So it is useful to use a special notation for this unique value, especially if we have a expression to calculate this unique value.

Definition 2.8. *Let $f: A \rightarrow B$ be a partial function then $(x, y) \in f$ is equivalent with $y = f(x)$*

From now on we will use the Axiom of Construction [axiom: 1.9] to define different classes related to partial functions without explicitly mentioning this. It is assumed that the reader understand when to use this axiom.

Definition 2.9. *Let $f: A \rightarrow B$ be a partial function then its domain noted as* $\mathrm{dom}(f)$ *and range noted as* $\mathrm{range}(f)$ *is defined by*

$$\mathrm{dom}(f) = \{x | \exists y \textit{ such that } (x, y) \in f\}$$

$$\mathrm{range}(f) = \{y | \exists x \textit{ such that } (x, y) \in f\}$$

Theorem 2.10. *If $f: A \rightarrow B$ is a partial function then* $\mathrm{dom}(f) \subseteq A$ *and* $\mathrm{range}(f) \subseteq B$

Proof. If $x \in \mathrm{dom}(f)$ then $\exists y$ such that $(x, y) \in f \underset{f \subseteq A \times B}{\Rightarrow} (x, y) \in A \times B$ proving that $x \in A$, hence

$$\mathrm{dom}(f) \subseteq A$$

Further if $y \in \mathrm{range}(f)$ then $\exists x$ such that $(x, y) \in f \underset{f \subseteq A \times B}{\Rightarrow} (x, y) \in A \times B$ proving that $y \in B$, hence

$$\mathrm{range}(f) \subseteq B$$

□

Corollary 2.11. *If A, B are sets and $f: A \rightarrow B$ a partial function then* $\mathrm{dom}(f)$ *and* $\mathrm{range}(f)$ *are sets*

Proof. Using [theorem: 2.10] we have that $\mathrm{dom}(f) \subseteq A$ and $\mathrm{range}(f) \subseteq B$, so applying the Axiom of Subsets [axiom: 1.54] proves that $\mathrm{dom}(f)$ and $\mathrm{range}(f)$ are sets. □

Definition 2.12. *Let $f: A \to B$ be a partial function and C a class such that $C \subseteq A$ then* ***the image of C by f*** *noted as $f(C)$ is defined by*

$$f(C) = \{y | \exists x \in C \text{ such that } (x, y) \in f\}$$

Remark 2.13. Note that we use a conflicting notation here. On one hand $y = f(x)$ can be interpreted as $(x, y) \in f$, on the other hand it can also means that y is the image of x by f. We adopt the following convention. If lower cases are used as in $y = f(x)$ we interpret this as $(x, y) \in f$ and if we use uppercase like in $f(C)$ we are talking about images. In case of doubt $(f)(C)$ always refers to the image.

Definition 2.14. *Let $f: A \to B$ be a partial function and C a class such that $C \subseteq B$ then* ***the preimage of C by f*** *noted as $f^{-1}(C)$ is defined by*

$$f^{-1}(C) = \{x | \exists y \in B \text{ such that } (x, y) \in f\}$$

Theorem 2.15. *Let $f: A \to B$ be a partial function, $C \subseteq A$ and $D \subseteq B$ then we have:*

1. $f(C) \subseteq \mathrm{range}(f)$
2. $f^{-1}(D) \subseteq \mathrm{dom}(f)$
3. $f(A) = \mathrm{range}(f)$
4. $f^{-1}(B) = \mathrm{dom}(f)$
5. *If $E \subseteq C$ then $f(E) \subseteq f(C)$*
6. *If $E \subseteq D$ then $f^{-1}(E) \subseteq f^{-1}(D)$*

and if in addition A, B are sets then $f(C)$ and $f^{-1}(D)$ are sets

Proof.

1. If $y \in f(C)$ then there exists a $x \in C$ such that $(x, y) \in f$, so $y \in \mathrm{range}(f)$. Hence
$$f(C) \subseteq \mathrm{range}(f)$$
2. If $x \in f^{-1}(D)$ then there exists a $y \in D$ such that $(x, y) \in f$, which proves that $x \in \mathrm{dom}(f)$, hence
$$f^{-1}(D) \subseteq \mathrm{dom}(f)$$
3. If $y \in \mathrm{range}(f)$ then $\exists x$ such that $(x, y) \in f$, which as $f \subseteq A \times B$ proves that $x \in A$, hence $y \in f(A)$, or $\mathrm{range}(f) \subseteq f(A)$. From (1) we have $f(A) \subseteq \mathrm{range}(f)$, so using [theorem: 1.8]
$$f(A) = \mathrm{range}(f)$$
4. If $x \in \mathrm{dom}(f)$ then $\exists y$ such that $(x, y) \in f$, which as $f \subseteq A \times B$ proves that $y \in B$, giving $x \in f^{-1}(B)$, hence $\mathrm{dom}(f) \subseteq f^{-1}(B)$. From (2) we have $f^{-1}(B) \subseteq \mathrm{dom}(f)$, so using [theorem: 1.8]
$$f^{-1}(B) = \mathrm{dom}(f)$$
5. If $y \in f(E)$ then $\exists x \in E$ such that $(x, y) \in f$, as $E \subseteq C$ we have $x \in C$ and still $(x, y) \in f$ so that $y \in f(C)$ proving
$$f(E) \subseteq f(C)$$
6. If $x \in f^{-1}(E)$ there $\exists y \in E$ such that $(x, y) \in f$, as $E \subseteq D$ we have $x \in D$ and still $(x, y) \in f$ so that $x \in f^{-1}(D)$ proving
$$f^{-1}(E) \subseteq f^{-1}(D)$$

Finally if A, B are sets then using [theorem: 2.11] $\mathrm{range}(f)$ and $\mathrm{dom}(f)$ are sets, applying then the Axiom of Subsets [axiom: 1.54] proves that $f(C)$ and $f^{-1}(D)$ are sets. $\square$

Next we define the composition of two partial functions.

Definition 2.16. *Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be two partial function then we define the composition of f and g noted as $g \circ f$ by*

$$g \circ f = \{z | z = (x, y) \text{ such that } \exists u \text{ with } (x, u) \in f \wedge (u, y) \in g\}$$

The above defines the graph of a new partial function as is expressed in the following theorem

Theorem 2.17. *Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be partial functions then $g \circ f: A \rightarrow C$ is a partial function.*

Proof. If $(x, y) \in g \circ f$ then there exist a u such that $(x, u) \in f$ and $(u, y) \in g$, as f, g are partial functions we have that $f \subseteq A \times B$ and $g \subseteq B \times C$. So $(x, u) \in A \times B$ and $(u, y) \in B \times C$. So $x \in A$ and $y \in C$ proving that $(x, y) \in A \times C$. Hence

$$g \circ f \subseteq A \times C$$

Further if $(x, y) \in g \circ f \wedge (x, y') \in g \circ f$ then there exists u, v such that $(x, u) \in f \wedge (u, y) \in g \wedge (x, v) \in f \wedge (v, y') \in g$. From $(x, u) \in f \wedge (x, v) \in f$ it follows [as f is a partial function] that $u = v$. So $(u, y) \underset{\text{u=v and [theorem: 1.43]}}{=} (u, y') \in g$. Hence as g is a partial function it follows that $y = y'$. To summarize

$$\text{If } (x, y) \in g \circ f \wedge (x, y') \in g \circ f \text{ then } y = y'$$

So all the requirements for $g \circ f: A \rightarrow C$ to be a partial function are satisfied. □

Theorem 2.18. (Associativity of Composition) *Let $f: A \rightarrow B$, $g: B \rightarrow C$ and $h: C \rightarrow D$ be functions then $h \circ (g \circ f) = (h \circ g) \circ f$*

Proof. If $(x.z) \in h \circ (g \circ f)$ then $\exists u$ such that $(x, u) \in g \circ f$ and $(u, z) \in h$. As $(x, u) \in g \circ f$ there exists a v such that $(x, v) \in f$ and $(v, u) \in g$. As $(v, u) \in g \wedge (u, z) \in h$ we have that $(v, z) \in h \circ g$, as $(x, v) \in f$ it follows $(x, z) \in (h \circ g) \circ f$.

If $(x, z) \in (h \circ g) \circ f$ there $\exists u$ such that $(x, u) \in f$ and $(u, z) \in h \circ g$. As $(u, z) \in h \circ g$ there $\exists v$ such that $(u, v) \in g$ and $(v, z) \in h$. From $(x, u) \in f$ and $(u, v) \in g$ we have that $(x, v) \in g \circ f$. As $(v, z) \in h$ we have that $(x, z) \in h \circ (h \circ f)$.

Using the Axiom of Extent [axiom: 1.5] it follows that

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

Let's look now at the domain and range of of the composition of two partial functions.

Theorem 2.19. *Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be partial functions then for $g \circ f: A \rightarrow C$ we have*

1. $\mathrm{dom}(g \circ f) = \mathrm{dom}(f) \bigcap f^{-1}(\mathrm{dom}(g))$
2. $\mathrm{range}(g \circ f) = g(\mathrm{range}(f) \bigcap \mathrm{dom}(g))$
3. $\mathrm{range}(g \circ f) \subseteq \mathrm{range}(g)$

Proof.

1. If $x \in \mathrm{dom}(g \circ f)$ then there exist a z such that $(x, z) \in g \circ f$. So there exist a y such that $(x, y) \in f$ and $(y, z) \in g$, hence $x \in \mathrm{dom}(f)$ and $y \in \mathrm{dom}(g) \underset{(x,y) \in f}{\Rightarrow} x \in f^{-1}(\mathrm{dom}(g))$. So $x \in \mathrm{dom}(f) \bigcap f^{-1}(\mathrm{dom}(g))$. Hence

$$\mathrm{dom}(g \circ f) \subseteq \mathrm{dom}(f) \bigcap f^{-1}(\mathrm{dom}(g)) \tag{2.10}$$

If $x \in \mathrm{dom}(f) \bigcap f^{-1}(\mathrm{dom} g))$ then $x \in \mathrm{dom}(f)$ so that $\exists y$ such that $(x, y) \in f$ and $x \in f^{-1}(\mathrm{dom}(g))$ so that $\exists y' \in \mathrm{dom}(g)$ such that $(x, y') \in f$. As f is a partial function it follows that $y = y'$. So $y \in \mathrm{dom}(g)$, from which it follows that $\exists z$ such that $(y, z) \in g$. As we have $(x, y) \in f$ and $(y, z) \in g$ it follows that $(x.z) \in g \circ f$ or $x \in \mathrm{dom}(g \circ f)$. This proves that $\mathrm{dom}(f) \bigcap f^{-1}(\mathrm{dom}(g)) \subseteq \mathrm{dom}(g \circ f)$, combining this with [eq: 2.10] allows us to use [theorem: 1.8] to get

$$\mathrm{dom}(g \circ f) = \mathrm{dom}(f) \bigcap f^{-1}(\mathrm{dom}(g))$$

2. If $z \in \mathrm{range}(g \circ f)$ then there exists a $x \in A$ such that $(x, z) \in g \circ f$, so there exist a y such that $(x, y) \in f \wedge (y, z) \in g$. Then $y \in \mathrm{range}(f)$ and $y \in \mathrm{dom}(g)$ or $y \in \mathrm{range}(f) \bigcap \mathrm{dom}(g)$, which as $(y, z) \in g$ proves that $z \in g(\mathrm{range}(f) \bigcap \mathrm{dom}(g))$. Hence

$$\mathrm{range}(g \circ f) \subseteq g\big(\mathrm{range}(f) \bigcap \mathrm{dom}(g)\big) \tag{2.11}$$

If $z \in g(\mathrm{range}(f) \bigcap \mathrm{dom}(g))$ then $\exists y \in \mathrm{range}(f) \bigcap \mathrm{dom}(g)$ such that $(y, z) \in g$. From $y \in \mathrm{range}(f)$ it follows that there exist a x such that $(x, y) \in f$. So $(x, z) \in g \circ f$ proving that $x \in \mathrm{range}(g \circ f)$, hence $g(\mathrm{range}(f) \bigcap \mathrm{dom}(g)) \subseteq \mathrm{range}(g \circ f)$. Combining this with [eq: 2.11] allows us to use [theorem: 1.8] to get

$$\mathrm{range}(g \circ f) = g\big(\mathrm{range}(f) \bigcap \mathrm{dom}(g)\big)$$

3. If $z \in \mathrm{range}(g \circ f)$ then there exists a x such that $(x, z) \in g \circ f$, so there exists a y such that $(x, y) \in f \wedge (y, z) \in g$. Hence $z \in \mathrm{range}(g)$ □

Theorem 2.20. *If $f: A \to B$ and $g: B \to C$ are partial functions then we have*

1. *If $C \subseteq A$ then $(g \circ f)(C) = g(f(C))$*
2. *If $D \subseteq B$ then $(g \circ f)^{-1}(D) = f^{-1}(g^{-1}(D))$*

Proof.

1. If $z \in (g \circ f)(C)$ then there exists a $x \in C$ such that $(x, z) \in g \circ f$. So by definition there exist a y such that $(x, y) \in f \wedge (y, z) \in g$. From $(x, y) \in f$ it follows that $y \in f(C)$ and as $(y, z) \in g$ it follows that $z \in g(f(C))$. Hence

$$(g \circ f)(C) \subseteq g(f(C)) \tag{2.12}$$

On the other hand if $z \in g(f(C))$ there exist a $y \in f(C)$ such that $(y, z) \in g$. As $y \in f(C)$ there exists a $x \in C$ such that $(x, y) \in f$. From $(x, y) \in f \wedge (y, z) \in g$ it follows that $(x, z) \in g \circ f$ so that [as $x \in C$] $z \in (g \circ f)(C)$. Proving $g(f(C)) \subseteq (g \circ f)(C)$, combining this with [eq 2.12] and [theorem: 1.8] gives

$$(g \circ f)(C) = g(f(C))$$

2. If $x \in (g \circ f)^{-1}(D)$ then there exist a $z \in D$ such that $(x, z) \in g \circ f$, hence $\exists y$ such that $(x, y) \in f \wedge (y, z) \in g$. So by definition $y \in g^{-1}(D)$ and as $(x, y) \in f$ it follows that $x \in f^{-1}(g^{-1}(D))$. Hence

$$(g \circ f)^{-1}(D) \subseteq f^{-1}(g^{-1}(D)) \tag{2.13}$$

If $x \in f^{-1}(g^{-1}(D))$ then there exist a $y \in g^{-1}(D)$ such that $(x, y) \in f$, as $y \in g^{-1}(D)$ then there exist a $z \in D$ such that $(y, z) \in g$. From $z \in D \wedge (x, y) \in f \wedge (y, z) \in g$ it follows that $x \in (g \circ f)^{-1}(D)$ proving that $f^{-1}(g^{-1}(D)) \subseteq (g \circ f)^{-1}(D)$. Combining this with [eq: 2.13] and [theorem: 1.8] gives

$$(g \circ f)^{-1}(D) = f^{-1}(g^{-1}(D))$$

□

2.2.2 Functions

Definition 2.21. *A partial function $f: A \to B$ is a **function** iff* $\mathrm{dom}(f) = A$

So every function is also a partial function, hence statements about partial functions applies also for functions.

Proposition 2.22. *A partial function $f: A \to B$ is a function iff $A \subseteq \mathrm{dom}(f)$*

Proof. As $A \subseteq \mathrm{dom}(f)$ and $\mathrm{dom}(f) \subseteq A$ [theorem: 2.10] we have by [theorem: 1.8] that

$$\mathrm{dom}(f) = A$$

□

Example 2.23. Let A, B be elements and define $f = \{(0, A), (1, B)\}$ then $f: \{0, 1\} \rightarrow \{A, B\}$ is a function

Proof. If $(x, y) \in f$ then

$$(x, y) = (0, A) \Rightarrow x = 1 \in \{0, 1\} \wedge y = A \in \{A, B\} \text{ so that } (x, y) \in \{0, 1\} \times \{A, B\}$$

or

$$(x, y) = (1, B) \Rightarrow x = 1 \in \{0, 1\} \wedge y = B \in \{A, B\} \text{ so that } (x, y) \in \{0, 1\} \times \{A, B\}$$

proving that

$$f \subseteq \{0, 1\} \times \{A, B\}$$

If $(x, y), (x, y') \in f$ then for (x, y) we have either:

$\boldsymbol{(x, y) = (0, A)}$**.** Then $x = 0$ and $y = A$ so that $(x', y') = (0, y') \in f \Rightarrow y' = A$ hence $y = y'$

$\boldsymbol{(x, y) = (1, B)}$**.** Then $x = 1$ and $y = B$ so that $(x', y') = (1, y') \in f \Rightarrow y' = B$ hence $y = y'$

which proves that

$$f: \{0, 1\} \rightarrow \{A, B\} \text{ is a partial function}$$

If $x \in \{0, 1\}$ then either $x = 0$ so that $(0, A) \in f$ or $x = 1$ so that $(1, B) \in f$, so $\{0, 1\} \subseteq \mathrm{dom}(f)$. Using [proposition: 2.22] it follows that

$$f: \{0, 1\} \rightarrow \{A, B\} \text{ is a function}$$ □

Next we define the class of all the graphs of functions between two classes

Note 2.24. Be aware that some books calls partial functions functions and functions mappings.

Definition 2.25. *Let A, B be two classes then we define the class B^A [using the Axiom of Construction] as*

$$B^A = \{f \mid f: A \rightarrow B \textit{ is a function}\}$$

Note 2.26. B^A is not the class of functions between A and B, but the class of graphs of functions between A and B. This distinction is important because it makes the following theorem possible.

Example 2.27. Let A be a class then $A^{\varnothing} = \{\varnothing\}$

Proof. Let $f \in A^{\varnothing}$ then $f: \varnothing \Rightarrow A$ is a function, so that $f \subseteq \varnothing \times A = \varnothing$ or $f = \varnothing$ □

Lemma 2.28. *If $f: A \rightarrow B$ is a function and $B \subseteq C$ then $f: A \rightarrow C$ is a function*

Proof. As $f: A \rightarrow B$ is a function we have $f \subseteq A \times B$ which as by [theorem: 1.48] $A \times B \subseteq A \times C$ means that $f \subseteq A \times C$'. Further as $f: A \rightarrow B$ is a function we we have also $\mathrm{dom}(f) = A$ and if (x, y), $(x, y') \in f$ then $y = y'$. So by definition$f: A \rightarrow C$ is a function. □

Theorem 2.29. *Let A, B, C be classes such that $B \subseteq C$ then $B^A \subseteq C^A$*

Proof. Let $f \in B^A$ then $f: A \rightarrow B$ is a function, using the above lemma [lemma: 2.28] we have that $f: A \rightarrow C$ is a function, hence $f \in C^A$ proving that

$$B^A \subseteq C^A$$ □

We have also the following relation between $A \times B$ and B^C

Theorem 2.30. *Let A, B be two classes then we have:*

1. $B^A \subseteq A \times B$
2. *If A, B are sets then B^A is a set*

Proof.

1. If $f \in B^A$ then $f: A \rightarrow B$ is a function so that $f \subseteq A \times B$ proving that $B^A \subseteq A \times B$
2. If A, B are sets then by [theorem: 1.67] we have that $A \times B$ is a set. So using the Axiom of Subsets [axiom: 1.54] we have that f is a set, □

Theorem 2.31. *Let A, B, C be classes then $A^C \bigcap B^C = (A \bigcap B)^C$*

Proof. First by [theorem: 1.25] we have $A \bigcap B \subseteq A$ and $A \bigcap B \subseteq B$ it follows from the above theorem [theorem: 2.29] that $(A \bigcap B)^C \subseteq A^C$ and $(A \bigcap B)^C \subseteq B^C$. Applying then [theorem: 1.26] gives

$$\left(A \bigcap B\right)^C \subseteq A^C \bigcap B^C \tag{2.14}$$

For the opposite inclusion, let $f \in A^C \bigcap B^C$ then $f \in A^C \wedge f \in B^C$ so that $f: C \rightarrow A$ and $f: C \rightarrow B$ are functions. Then we have that $f \subseteq C \times A$ and $f \subseteq C \times B$ so that

$$f \subseteq (C \times A) \bigcap (C \times B) \underset{1.49}{=} \left(C \bigcap C\right) \times \left(A \bigcap B\right) \underset{[\text{theorem: } 1.30]}{=} C \times \left(A \bigcap B\right)$$

Further as $f: A \rightarrow C$ is a function we have $(x, y), (x, y') \in f$ and $\operatorname{dom}(f) = C$ so that

$$f: C \rightarrow \left(A \bigcap B\right) \text{ is a function}$$

proving that $f \in (A \bigcap B)^I$. So $A^C \bigcap B^C \subseteq (A \bigcap B)^C$ which combined with [eq: 2.14] gives

$$A^C \bigcap B^C = \left(A \bigcap B\right)^C$$

□

We have the follow trivial fact about a function

Proposition 2.32. *Let $f: A \rightarrow B$ be a function then if $\operatorname{range}(f) \subseteq C$ we have that $f: A \rightarrow C$ is a function.*

Proof. If $(x, y) \in f$ then $y \in \operatorname{range}(f)$ hence as $\operatorname{range}(f) \subseteq C$ $y \in C$. As $f \subseteq A \times B$ we have also $x \in A$ so that $(x, y) \in C \times B$. Hence $f \subseteq A \times C$, further if $(x, y), (x, y') \in f$ we have as $f: A \rightarrow B$ is a function that $y = y'$. So

$$f: A \rightarrow C \text{ is a partial function}$$

As $\operatorname{range}(f) = A$ (because $f: A \rightarrow B$ is a function] we have that $f: A \rightarrow C$ a function □

We have the following trivial proposition about the equality of two functions

Proposition 2.33. *Two functions $f: A \rightarrow B$ and $g: A \rightarrow B$ are equal if*

$$[(x, y) \in f \Rightarrow (x, y) \in g \wedge (x, y) \in g \Rightarrow (x, y) \in f]$$

Proof. Note that the statement $f: A \rightarrow B$ and $g: A \rightarrow B$ are equal is equivalent with $\langle A, B, f\rangle = \langle A, B, g\rangle$, which by 2.5 is equivalent with $A = A \wedge B = B \wedge f = g$, As $A = A$ and $B = B$ are true this is equivalent with $f = g$. Now by the Axiom of Extent [axiom: 1.5] we have that

$$f = g \Leftrightarrow [(x, y) \in f \Rightarrow (x, y) \in g \wedge (x, y) \in g \Rightarrow (x, y) \in f]$$

□

If $f: A \rightarrow B$ is a function then for every $x \in A$ we have a unique $y \in B$ such that $(x, y) \in f$. Furthermore in many cases we have actually a expression valid for every $x \in A$ to calculate this unique value. To express this we use the following notation.

Definition 2.34. *If $f: A \rightarrow B$ is a function then*

$$\boldsymbol{y = f(x)} \text{ or } \boldsymbol{f(x) = y} \text{ is equivalent with } \boldsymbol{(x, y) \in f}$$

and

$$\boldsymbol{f(x)=E(x)} \text{ where } \boldsymbol{E(x)} \text{ is a expression depending on } \boldsymbol{x} \text{ is equivalent with } \boldsymbol{(x,E(x))\in f}$$

Further if $D\subseteq B$ then $\boldsymbol{f(x)\in D}$ *is the same as* $\boldsymbol{\exists y\in D}$ ***such that*** $\boldsymbol{y=f(x)}$ ***or*** $\boldsymbol{(x,y)\in f}$

Example 2.35. Let $3\cdot x+1$ be the value associated with x, so $f=\{z|z=(x,3\cdot x+1)\in f\wedge x\in A\}$, then we can use the following equivalent notations to define our function

$$f\colon A\rightarrow B \text{ is defined by } x\rightarrow 3\cdot x+1$$

If we have defined a function $f\colon A\rightarrow B$ using a expression and we want to refer to the expression of the function we use the notation $f(x)$. Hence we define a function also as

$$f\colon A\rightarrow B \text{ is defined by } x\rightarrow f(x)=3\cdot x+1$$

or

$$f\colon A\rightarrow B \text{ is defined by } x\rightarrow f(x) \text{ where } f(x)=3\cdot x+1$$

or

$$f\colon A\rightarrow B \text{ is defined by } f(x)=3*x+1$$

In all of the above cases we actually means that $\langle f,A,B\rangle$ is a function with $f=\{z|z=(x,3\cdot x+1)\wedge x\in A\}$.

Using the above notation we can reformulate [proposition: 2.33] in a form that is easier to work with if we use expressions to define a function.

Proposition 2.36. *Two functions $f\colon A\rightarrow B$ and $g\colon A\rightarrow B$ are equal if and only if*

$$\forall x\in A\ f(x)=g(x)$$

Proof. Assume that $f\colon A\rightarrow B$ and $g\colon A\rightarrow B$ are equal then if $x\in A$ we have $\exists y\in B$ such that $(x,y)\in f$ or $y=f(x)$, using [proposition: 2.33] we have also $(x,y)\in g$ hence $y=g(x)$ which proves that $f(x)=g(x)$.

On the other hand assume that $\forall x\in A\ f(x)=g(x)$ then if $(x,y)\in f$ we have $y=f(x)=g(x)$ so that $(x,y)\in g$. If $(x,y)\in g$ then $y=g(x)=f(x)$ or $(x,y)\in g$. Using [proposition: 2.33] we have then that $f\colon A\rightarrow B$ and $g\colon A\rightarrow B$ are equal. □

Using the new notation, composition of function is written as

Theorem 2.37. *If $f\colon A\rightarrow B$ and $g\colon B\rightarrow C$ are two functions then*

$$(g\circ f)(x)=g(f(x))$$

Proof. Take $z=(g\circ f)(x)$ then $(x,z)\in g\circ f$ so that $\exists y$ such that $(x,y)\in f$ and $(y,z)\in g$. Hence $y=f(x)$ and $z=g(y)$ so that $z=g(f(x))$, proving $(g\circ f)(x)=g(f(x))$. □

Image and pre-image can also be expressed in the new notation.

Proposition 2.38. *Let $f\colon A\rightarrow B$ a function, $C\subseteq A$ and $D\subseteq B$ then*

1. *$y\in f(C)\Leftrightarrow\exists x\in A$ such that $y=f(x)$*
2. *$x\in f^{-1}(D)\Leftrightarrow f(x)\in D$*

Proof.

1.

$$\begin{aligned} y\in f(C) &\Leftrightarrow \exists x\in C \text{ such that } (x,y)\in f\\ &\Leftrightarrow \exists x\in C \text{ such that } y=f(x) \end{aligned}$$

2.

$$\begin{aligned} x \in f^{-1}(C) &\Leftrightarrow \exists y \in D \text{ such that } (x, y) \in f \\ &\Leftrightarrow \exists y \in D \text{ such that } y = f(x) \\ &\Leftrightarrow f(x) \in D \end{aligned}$$

□

Let's now look at some example of functions:

Example 2.39. (Empty Function) $\varnothing: \varnothing \rightarrow B$

Proof. First $\varnothing \subseteq \varnothing \times B$ by [theorem: 1.18], if $x \in \mathrm{dom}(\varnothing)$ then $\exists y \in \varnothing$ such that $(x, y) \in \varnothing$ which is a contradiction, so by [theorem: 1.19] we have that $\mathrm{dom}(\varnothing) = \varnothing$. And finally $(x, y) \in \varnothing \wedge (x, y') \in \varnothing \Rightarrow y = y'$ is satisfied vacuously as $(x, y) \in \varnothing \wedge (x, y') \in \varnothing$ is never true. □

Example 2.40. (Constant Function) Let A, B classes and $c \in B$ then $C_c: A \rightarrow B$ is defined by $C_c(x) = c$ or formally $C_c = \{z | z = (x, c) | x \in A\} = A \times \{c\}$

Proof. If $(x, y) \in C_c$ then $x \in A$ and $y = c \in B$ so that $C_c \subseteq A \times B$. If $(x, y) \in C_c \wedge (x, y') \in C_c$ then $y = c \wedge y' = c$ so that $y = y'$. So

$$C_c: A \rightarrow B \text{ is a partial function}$$

Finally if $x \in A$ then $(x, c) \in C_c$ so that $A \subseteq \mathrm{dom}(C_c)$ which by [proposition: 2.22] proves that

$$C_c: A \rightarrow B \text{ is } a \text{ function}$$

□

Example 2.41. (Characteristics Function) Let A be a class and $B \subseteq A$ then $\mathcal{X}_{A,B}: A \rightarrow \{0, 1\}$ is defined by $\mathcal{X}_{A,B} = (B \times \{1\}) \bigcup ((A \setminus B) \times \{0\})$ [so that $\mathcal{X}_{A,B}(x) = \left\{ \begin{smallmatrix} 1 \text{ if } x \in B \\ 0 \text{ if } x \in A \setminus B \end{smallmatrix} \right.$

Proof. If $(x, y) \in \mathcal{X}_{A,B}$ then either $(x, y) \in (B \times \{1\}) \Rightarrow x \in B \underset{B \subseteq A}{\Rightarrow} x \in A$ and $y = 1 \in \{0, 1\}$ or $(x, y) \in ((A \setminus B), \{0\}) \Rightarrow x \in A \setminus B \Rightarrow x \in A$ and $y = 1 \in \{0, 1\}$ so that

$$\mathcal{X}_{A,B} \subseteq A \times \{0, 1\}$$

Also if $(x, y), (x, y') \in \mathcal{X}_{A,B}$ then for (x, y) we have either:

$\boldsymbol{(x, y) \in B \times \{1\}}$**.** then $x \in B$ so that $(x, y') \in B \times \{1\}$ hence $y = 1 = y'$

$\boldsymbol{(x, y) \in (A \setminus B) \times \{0\}}$**.** then $x \in A \setminus B$ so that $(x, y') \in (A \setminus B) \times \{0\}$ hence $y = 0 = y'$

or in all cases $y = y'$ and $x \in B \bigcup (A \setminus B) = A$. Hence $\mathcal{X}_{A,B}: A \rightarrow \{0, 1\}$ is a function. □

Example 2.42. (Identity Function) Let A be a class then $\mathrm{Id}_A: A \rightarrow A$ is defined by

$$I_A = \{z | z = (x, x) \wedge x \in A\}$$

Proof. Trivially we have $\mathrm{Id}_A \subseteq A \times A$. If $(x, y), (x, y') \in \mathrm{Id}_A$ then $(x, y) = (x, x) = (x, y')$ proving that $y = x = y'$. Hence $I_d: A \rightarrow A$ is a partial function. Further if $x \in A$ then $(x, x) \in \mathrm{Id}_A$ so that $x \in \mathrm{dom}(\mathrm{Id}_A)$ or $\mathrm{dom}(\mathrm{Id}_A) \subseteq A$ which by [proposition: 2.22] proves that

$$\mathrm{Id}_A: A \rightarrow A \text{ is a function}$$

□

Proposition 2.43. *Let $f: A \rightarrow B$ be a partial function then $f = f \circ \mathrm{Id}_A$ and $f = \mathrm{Id}_B \circ f$*

Proof.

1. If $(x, y) \in f$ then as $f \subseteq A \times B$ we have $x \in A \wedge x \in B$, by the definition of Id_A we have $(x, x) \in \mathrm{Id}_A$, as $(x, y) \in f$ we have $(x, y) \in \mathrm{Id}_A \circ f$. If $(x, y) \in f \circ \mathrm{Id}_A$ then $\exists x'$ such that $(x, x') \in \mathrm{Id}_A \wedge (x', y) \in f$. By definition of Id_A we have that $\exists z \in A$ such that $(x, x') = (z, z)$ hence $x = x'$ so that $(x, y) \in f$. Using the Axiom of Extent [axiom: 1.5] we have then that

$$f = f \circ \mathrm{Id}_A$$

2. If $(x,y)\in f$ then as $f\subseteq A\times B$ we have $x\in A\wedge x\in B$, by the definition of Id_B we have $(y,y)\in\mathrm{Id}_B$, so $(x,y)\in\mathrm{Id}_B\circ f$. If $(x,y)\in\mathrm{Id}_B\circ f$ then $\exists y'$ such that $(x,y')\in f\wedge(y,y')$, from the definition of Id_B we have that $y=y'$ so that $(x,y)\in f$. Using the Axiom of Extent [axiom: 1.5] we have then that
$$f=\mathrm{Id}_B\circ f$$
□

As a function $f\colon A\rightarrow B$ is a partial function with $\mathrm{dom}(f)=A$ we can refine [theorem: 2.15].

Theorem 2.44. *If $f\colon A\rightarrow B$ is a function $C\subseteq B$ and $D\subseteq B$ then we have*

1. $f(C)\subseteq B$
2. $f^{-1}(D)\subseteq A$
3. $f(A)=\mathrm{range}(f)$
4. $f^{-1}(B)=A$

Proof. This follows from 2.15 taking in account that $A=\mathrm{dom}(f)$ □

Next we proof that the composition of two functions is again a function

Theorem 2.45. *Let $f\colon A\rightarrow B$ and $g\colon B\rightarrow C$ functions then $g\circ f\colon A\rightarrow C$ is also a function with* $\mathrm{range}(f)=g(\mathrm{range}(f))$

Proof. Using [theorem: 2.17] we have that
$$g\circ f\colon A\rightarrow C \text{ is a partial function}$$
Further using [theorem: 2.19] we have
$$\begin{aligned}\mathrm{dom}(g\circ f) &= \mathrm{dom}(f)\bigcap f^{-1}(\mathrm{dom}(g))\\ &\underset{f,g\text{ are functions}}{=} A\bigcap f^{-1}(B)\\ &\underset{\text{[theorem: 2.44}}{=} A\end{aligned}$$
which proves that
$$g\circ f \text{ is a function}$$
Finally
$$\begin{aligned}\mathrm{range}(g\circ f) &\underset{\text{[theorem: 2.19}}{=} g\big(\mathrm{range}(f)\bigcap \mathrm{dom}(g)\big)\\ &\underset{f\text{ is a function}}{=} g\big(\mathrm{range}(f)\bigcap B\big)\\ &\underset{\mathrm{range}(f)\subseteq B\text{ [theorem: 2.10]}}{=} g(\mathrm{range}(f))\end{aligned}$$
□

2.2.3 Injectivity, Surjectivity and bijectivity

First we define injectivity and surjectivity of partial functions.

Definition 2.46. *Let $f\colon A\rightarrow B$ be a partial function then we say that:*

1. *f is* ***injective*** *iff if* $(x,y)\in f\wedge(x',y)\in f$ *implies* $x=x'$
2. *f is* ***surjective*** *iff* $\mathrm{range}(f)=B$

Proposition 2.47. *A partial function $f\colon A\rightarrow B$ is surjective if $B\subseteq\mathrm{range}(f)$*

Proof. By [theorem: 2.10] $\mathrm{range}(f)\subseteq B$, so if $B\subseteq\mathrm{range}(f)$ it follows from [theorem: 1.8] that $B=\mathrm{range}(f)$, proving surjectivity. □

Using the notation $y = f(x)$ is the same as $(x, y) \in f$ we have

Theorem 2.48. *Let $f: A \to B$ be a function then*

1. *f is injective if and only if $\forall x, x \in A$ with $f(x) = f(x')$ we have $x = x'$*
2. *If $B \subseteq C$ and $f: A \to B$ is injective then $f: A \to C$ is injective*
3. *f is surjective if and only if $\forall y \in B$ there exists a $x \in A$ such that $y = f(x)$*

Proof.

1.
   - **⇒.** Let $x, x' \in A$ then if $y = f(x) = f(x')$ we have $(x, y) \in f$ and (x', y) so that $x = x'$
   - **⇐.** If $(x, y) \in f$ and $(x', y) \in f$ then $y = f(x) \wedge y = f(x')$ so that $f(x) = f(x')$ so that $x = x'$
2. This is trivial because injectivity is a property of the graph of a function.
3.
   - **⇒.** As $B = \mathrm{range}(f)$ we have $y \in B$ then $\exists x$ such that $(x, y) \in f \Rightarrow y = f(x)$ which as $f \subseteq A \times B$ proves that $x \in A$. So $\forall y \in B$ $\exists x \in A$ such that $y = f(x)$
   - **⇐.** Let $y \in B$ then $\exists x \in A$ such that $y = f(x)$ or $(x, y) \in f$ proving that $B \subseteq \mathrm{range}(f)$, using [proposition: 2.47] we have that f is surjective □

Example 2.49. Let A, B be classes, $B \subseteq A$ then $i_B: B \to A$ defined by $i_B = \{(x, x) | x \in B\}$ is a injective function. This function is called the **inclusion** function.

Proof. First if $(x, y) \in i_B$ then $\exists b \in B$ such that $(x, y) = (b, b)$ so that $x = b \in B \wedge y = b \in B \subseteq A$ proving that

$$i_B \subseteq B \times A$$

Further if $(x, y), (x, y') \in i_B$ then $\exists b, b' \in B$ such that $(x, y) = (b, b) \wedge (x, y') = (b', b')$, so that $x = b \wedge y = b \wedge x = b' \wedge y' = b'$, hence $y = y'$. So

$$i_B: B \to A \text{ is a partial function}$$

If $x \in B$ then $(x, x) \in i_B$ proving that $A \subseteq \mathrm{dom}(i_b)$ so using [proposition: 2.22] it follows that

$$i_B: B \to A \text{ is a function}$$

Finally if $(x, y), (x', y) \in i_B$ then there exists $b, b' \in B$ such that $(x, y) = (b, b) \wedge (x', y) = (b', b')$, so that $x = b \wedge y = b \wedge x' = b' \wedge y = b'$, hence $x = x'$, proving injectivity.

□

The following axiom ensures that the image of a set by a surjection is a set.

Axiom 2.50. (Axiom of Replacement) *If A is a set and $f: A \to B$ a surjection then B is a set.*

Proposition 2.51. *If $f: A \to B$ is a a function and $C \subseteq A, D \subseteq B$ then*

1. *$C \subseteq f^{-1}(f(C))$*
2. *If f is injective then $C = f^{-1}(f(C))$*
3. *If f is surjective then $D = f(f^{-1}(D))$*

Proof.

1. Let $x \in C$ then, as f is a function, $A = \mathrm{dom}(f)$, so there exists a y such that $(x, y) \in f$ proving that $y \in f(C)$, hence $x \in f^{-1}(f(C))$. So

$$C \subseteq f^{-1}(f(C))$$

2. If $x \in f^{-1}(f(C))$ then $\exists y \in f(C)$ such that $(y, x) \in f^{-1}$, hence $(x, y) \in f$. As $y \in f(C)$ there exists a $x' \in C$ such that $(x', y) \in f$. Given that f is injective it follows from $(x, y), (x', y) \in f$ that $x = x'$, so as $x' \in C$ it follow that $x \in C$. Hence $f^{-1}(f(C)) \subseteq C$ which combined with (1) proves
$$C = f^{-1}(f(C))$$

3. If $y \in f(f^{-1}(D))$ then $\exists x \in f^{-1}(D)$ such that $(x, y) \in f$, hence $\exists z \in D$ such that $(z, x) \in f^{-1} \Rightarrow (x, z) \in f$, As f is a function we have $y = z$ so that $y \in D$. Hence
$$f(f^{-1}(D)) \subseteq D \tag{2.15}$$
If $y \in D$ then as f is a surjection there exist a $x \in A$ such that $(x, y) \in f$, hence $x \in f^{-1}(D)$ proving that $y \in f(f^{-1}(D))$. So $D \subseteq f(f^{-1}(D))$ which together with [eq: 2.15] proves
$$D = f(f^{-1}(D))$$
□

The importance of injectivity is that it allows us to define the inverse of a partial function. First we define the inverse graph of the graph of a partial function.

Definition 2.52. *Let $f: A \rightarrow B$ be a partial function then the* ***inverse of the graph f*** *noted as f^{-1} is defined by*
$$f^{-1} = \{z : z = (z, y) \text{ where } (y, x) \in f\}$$

Theorem 2.53. *Let $f: A \rightarrow B$ be a* **injective** *partial function then $f^{-1}: B \rightarrow A$ is a partial function*

Proof. If $(x, y) \in f^{-1}$ then $(y, x) \in f$ which, as $f \subseteq A \times B$, gives $(y, x) \in A \times B$, so $x \in B \wedge y \in A$, proving $(x, y) \in B \times Y$. Hence
$$f^{-1} \subseteq B \times A$$
Further if $(x, y) \in f^{-1}$ and $(x, y') \in f^{-1}$ then $(y, x) \in f \wedge (y, x') \in f$ which, as f is injectivity proves that $y = y'$. So all the conditions are satisfied to make $f^{-1}: B \rightarrow A$ a partial function. □

Note 2.54. The requirement that f is injective is needed to make f^{-1} is a partial function. For example assume that $A = \{1, 2, 3\}$, $B = \{10, 20\}$ and $f = \{(1, 10), (2, 10), (3, 20)\}$ then $f^{-1} = \{(10, 1), (10, 2), (20, 3)\}$ which is not the graph of a partial function.

If f is a injective function then the above theorem ensures that f^{-1} is a partial function however f^{-1} can be a graph of a function if we restrict the source of the inverse function.

Theorem 2.55. *If $f: A \rightarrow B$ is a injective function then $f^{-1}: f(A) \rightarrow A$ is a function*

Proof. First if $(x, y) \in f^{-1}$ then $(y, x) \in f \subseteq A \times B$ so that $y \in A \wedge x \in B$, as $(y, x) \in f$ we have that $x \in f(A)$, hence $(x, y) \in f(A) \times A$. So $f^{-1} \subseteq f(A) \times B$. Further if $(x, y), (x, y') \in f^{-1}$ then $(y, x), (y', x) \in f$ which as f is injective proves $y = y'$. Hence
$$f^{-1}: f(A) \rightarrow A \text{ is a partial function}$$
Further if $x \in f(A)$ then there exists a $y \in A$ such that $(y, x) \in f$, hence $(x, y) \in f^{-1}$ so that $x \in \text{dom}(f^{-1})$, proving that $f(A) \subseteq \text{dom}(f^{-1})$. Hence
$$f^{-1}: f(A) \rightarrow A \text{ is a function}$$
□

Corollary 2.56. *If $f: A \rightarrow B$ is a function, $A \neq \varnothing$ then $f: A \rightarrow B$ is injective if and only if there exist a function $g: B \rightarrow A$ such that $g \circ f = \text{Id}_A$*

Proof.

⇒. Using the above [theorem: 2.55] we have that $f^{-1}: f(A) \rightarrow A$ is a function. As $A \neq 0$ there exist a $a \in A$ so we can consider the constant function $C_a: B \setminus f(A) \rightarrow A$ [see example: 2.40]. As $f(A) \bigcap (B \setminus f(A)) = \varnothing$ and $B = f(A) \bigcup (B \setminus f(A))$ we have by [theorem: 2.73] that
$$g = C_a \bigcup f^{-1} : B \rightarrow A$$

is a function. If $(x, y) \in g \circ f$ then $\exists$z such that $(x, z) \in f \wedge (z, y) \in g$. As $(x, z) \in f$ we have that $(z, x) \in f^{-1} \subseteq C_a \bigcup f^{-1} = g$, as also $(z, y) \in g$ and g is function, we have that $y = x$ so that $(x, y) = (x, x) \in \mathrm{Id}_A$ hence

$$g \circ f \subseteq \mathrm{Id}_A$$

Further if $(x, y) \in \mathrm{Id}_A$ then $x = y$, as $x \in A = \mathrm{dom}(f)$ there exist a $z \in B$ such that $(x, z) \in f \Rightarrow (z, x) \in f^{-1} \subseteq C_a \bigcup f^{-1} = g$ proving that $(x, y) = (x, x) \in g \circ f$. Hence

$$\mathrm{Id}_A \subseteq g \circ f$$

proving that

$$g \circ f = \mathrm{Id}_A$$

$\Leftarrow$**.** Assume that there exists a function $g: B \rightarrow A$ such that $g \circ f = \mathrm{Id}_A$ then

$$\begin{array}{rcl} (x, y), (x', y) \in f \subseteq A \times B & \underset{y \in B, \mathrm{dom}(g) = B}{\Rightarrow} & \exists z \vdash (y, z) \in g \\ & \Rightarrow & (x, z), (x', z) \in g \circ f = \mathrm{Id}_A \\ & \Rightarrow & x = z = x' \\ & \Rightarrow & x = x' \end{array}$$

□

Definition 2.57. *A function $f: A \rightarrow B$ is a **bijection** iff the function is **injective** and **surjective**.*

Definition 2.58. *Two classes A and B are bijective iff there exists a bijection between A and B*

Example 2.59. The function $\varnothing: \varnothing \rightarrow \varnothing$ is a bijection.

Proof. By [example: 2.39] $\varnothing: \varnothing \rightarrow \varnothing$ is a function. To prove that is a bijection we have:

injectivity. $\forall (x, y), (x', y) \in \varnothing$ we have $x = x'$ is satisfied vacuously.

surjectivity. $\forall y \in \varnothing$ there exist a $x \in \varnothing$ such that $(x, y) \in \varnothing$ is satisfied vacuously. □

Example 2.60. Let A be a class then $\mathrm{Id}_A: A \rightarrow A$ [example: 2.42] is a bijection

Proof. Let $(x, y) \in \mathrm{Id}_A \wedge (x', y) \in \mathrm{IdA}$ then $\exists z, z' \in A$ such that $(x, y) = (z, z) \wedge (x', y) = (z', z')$. So using [theorem: 1.43] $x = z \wedge y = z \wedge x = z' \wedge y = z'$. Using [theorem: 1.8] repeatedly gives then $x = x'$ proving that

$$\mathrm{Id}_A \text{ is injective}$$

If $y \in A$ then by definition $(y, y) \in \mathrm{Id}_A$ so that $\mathrm{range}(\mathrm{Id}_A) \subseteq A$. Using [theorem: 2.47] it follows that

$$\mathrm{Id}_A \text{ is surjective}$$ □

Example 2.61. Let $I = \{0\}$ B a class and take $f: I \rightarrow \{B\}$ defined by $f = \{(0, B)\}$ is a bijection

Proof. As $0 \in \{0\}$ and $B \in \{B\}$ it follows that $(0, B) \in \{0\} \times \{B\}$, hence $f = \{(0, B)\} \subseteq \{0\} \times \{B\}$. If $(x, y), (x, y') \in f = \{0\} \times \{B\}$ then $y = B = y'$, further $\mathrm{dom}(f) = \{0\} = I$. So we conclude that $f: \{0\} \rightarrow \{B\}$ is indeed a function. Further if $y \in \{B\}$ then $y = B$ and as $(0, B) \in f$ it follows that $y \in \mathrm{range}(f)$ or $\{B\} \subseteq \mathrm{range}(f)$, which by [theorem: 2.47] proves that f is surjective. Finally if $(x, y), (x', y) \in f = \{(0, B)\}$ then $x = 0 = x'$ proving that $f: \{0\} \rightarrow \{B\}$ is a bijection. □

Proposition 2.62. *If $f: A \rightarrow B$ is a injective function then $f: A \rightarrow f(A)$ is a bijection*

Proof. As injectivity is a property of the graph of a function, the function $f: A \rightarrow B$ is still injective. Further $\mathrm{range}(f) \underset{\text{[theorem: 2.15]}}{=} f(A)$ which proves surjectivity. □

Theorem 2.63. If *$f: A \rightarrow B$ is a bijection then $f^{-1}: B \rightarrow A$ is a function*

Proof. As $f: A \rightarrow B$ is injective and surjective we have that $f(A) = B$ and by [theorem: 2.55] that $f^{-1}: f(A) \rightarrow B$ is a function. Hence $f^{-1}: B \rightarrow A$ is a function. □

Theorem 2.64. *If $f: A \rightarrow B$ is bijective then*

1. $f \circ f^{-1} = \mathrm{Id}_B$
2. $f^{-1} \circ f = \mathrm{Id}_A$

Proof. First $f^{-1}: B \rightarrow A$ is a function by [theorem: 2.63].

1. Let $(x, y) \in f \circ f^{-1}$ then $\exists z$ such that $(x, z) \in f^{-1} \Rightarrow (z, x)$ and $(z, y) \in f$. As f^{-1} is the graph of a function we have that $x = y$. Further from $(x, z) \in f^{-1} \subseteq B \times A$ it follow that $x \in B$. Hence $(x, y) = (x, x) \in \mathrm{Id}_B$, proving that

$$f \circ f^{-1} \subseteq \mathrm{Id}_B \tag{2.16}$$

If $(x, y) \in \mathrm{Id}_B$ then $\exists z \in B$ such that $(x, y) = (z, z)$ so that $x = y \in B$, As $B = \mathrm{dom}(f^{-1})$ there exists a u such that $(y, u) \in f^{-1} \Rightarrow (u, y) \in f$ so that $(y, y) \in f \circ f^{-1} \underset{x=y}{\Rightarrow} (x, y) \in f \circ f^{-1}$. So $\mathrm{Id}_B \subseteq f \circ f^{-1}$. Combining this with [eq: 2.16] proves that

$$f \circ f^{-1} = \mathrm{Id}_B$$

2. Let $(x, y) \in f^{-1} \circ f$ then $\exists z$ such that $(x, z) \in f \Rightarrow (z, x) \in f^{-1}$ and $(z, y) \in f^{-1}$. As f^{-1} is the graph of a function we have that $x = y$. Further from $(x, z) \in f \subseteq A \times B$ it follows that $x \in A$. Hence $(x, y) = (x, x) \in \mathrm{Id}_A$, proving that

$$f^{-1} \circ f \subseteq I_A \tag{2.17}$$

If $(x, y) \in \mathrm{Id}_A$ then $\exists z \in A$ such that $(x, y) = (z, z)$ so that $x = y \in A$, As $A = \mathrm{dom}(f)$ there exists a u such that $(x, u) \in f \Rightarrow (u, x) \in f^{-1}$ so that $(x, x) \in f^{-1} \circ f \underset{x=y}{\Rightarrow} (x, y) \in f^{-1} \circ f$. So $\mathrm{Id}_B \subseteq f^{-1} \circ f$. Combining this with [eq: 2.17] proves that

$$f^{-1} \circ f = \mathrm{Id}_A$$

□

Corollary 2.65. *If $f: A \rightarrow B$ is bijection then*

1. $\forall x \in A$ *we have* $(f^{-1})(f(x)) = x$
2. $\forall y \in B$ *we have* $f((f^{-1})(y)) = y$

Proof.

1. If $x \in A$ then $(f^{-1})(f(x)) = ((f^{-1}) \circ f)(x) \underset{\text{[theorem:}}{=} \mathrm{Id}_A(x) = x$
2. If $y \in B$ then $f((f^{-1})(y)) \underset{\text{[theorem:}}{=} \mathrm{Id}_B(y) = y$ □

Corollary 2.66. *Let $f: A \rightarrow B$ a function then the following are equivalent:*

1. $f: A \rightarrow B$ *is a bijection*
2. *There exists a function $g: B \rightarrow A$ such that $f \circ g = \mathrm{id}_B$ and $g \circ f = \mathrm{Id}_A$*

Proof.

1 ⇒ 2. This follows from [theorem: 2.64] by taking $g = f^{-1}$

2 ⇒ 1. Let $(x, y), (x', y) \in f \subseteq A \times B$, as $y = \mathrm{dom}(g)$ there exists a z such that $(y, z) \in g$, hence $(x, z), (x', z) \in g \circ f = \mathrm{Id}_A$ so that $x = z = x'$ proving that

$$f: A \rightarrow B \text{ is injective}$$

Further if $y \in B$ then $(y, y) \in \mathrm{Id}_B = f \circ g$ so there exists a $z \in A$ such that $(y, z) \in g$ and $(z, y) \in f$. Proving that $B \subseteq \mathrm{range}(f)$ so by [proposition: 2.47]

$$f: A \rightarrow B \text{ is a surjection}$$

□

The inverse of a bijection is again a bijection

Corollary 2.67. *If $f: A \rightarrow B$ is a bijection then $f^{-1}: B \rightarrow A$ is a bijection*

Proof. If $f: A \rightarrow B$ is a bijection then by [theorem: 2.64] $f \circ f^{-1} = \mathrm{Id}_B$ and $f^{-1} \circ f = \mathrm{Id}_A$ which by [theorem: 2.66] proves that $f^{-1}: B \rightarrow A$ is a bijection. □

Proposition 2.68. *If $f: A \rightarrow B$ is a bijection then we have:*

1. *If $g: B \rightarrow A$ is such that $f \circ g = \mathrm{Id}_B$ and $g \circ f = \mathrm{Id}_A$ then $g = f^{-1}$*
2. $(f^{-1})^{-1} = f$

Proof.

1. We have

$$\begin{aligned} f \circ g = \mathrm{Id}_B \quad & \Rightarrow \quad f^{-1} \circ (f \circ g) = f^{-1} \circ \mathrm{Id}_B \\ & \underset{\text{[proposition: 2.43}}{\Rightarrow} \quad f^{-1} \circ (f \circ g) = f^{-1} \\ & \underset{\text{[theorem: 2.18]}}{\Rightarrow} \quad (f^{-1} \circ f) \circ g = f^{-1} \\ & \underset{\text{[function: 2.64]}}{\Rightarrow} \quad \mathrm{Id}_B \circ g = f^{-1} \\ & \underset{\text{[proposition: 2.43}}{\Rightarrow} \quad g = f^{-1} \end{aligned}$$

2. We have

$$\begin{aligned} (x, y) \in (f^{-1})^{-1} \quad & \Leftrightarrow \quad (y, x) \in f^{-1} \\ & \Leftrightarrow \quad (x, y) \in f \end{aligned}$$

which by the Axiom of Extent [axiom: 1.5] proves

$$(f^{-1})^{-1} = f$$ □

Composition preserves injectivity, surjectivity and bijectivity

Theorem 2.69. *If A, B and C are classes then we have*

1. *If $f: A \rightarrow B$ and $g: B \rightarrow C$ are injective partial functions then $g \circ f: A \rightarrow C$ is a injective partial function*
2. *If $f: A \rightarrow B$ and $g: B \rightarrow C$ are surjective partial functions then $g \circ f: A \rightarrow C$ is a surjective partial function*
3. *If $f: A \rightarrow B$ and $g: B \rightarrow C$ are bijective functions then $g \circ f: A \rightarrow C$ is a bijective function*
4. *If $f: A \rightarrow B$ and $g: B \rightarrow C$ are bijective functions then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$*

Proof.

1. Let $(x, z), (x', z) \in g \circ f$ then $\exists u, v$ such that

$$(x, u) \in f \wedge (x', v) \in f \wedge (u, y) \in g \wedge (v, y) \in g$$

As g is injective we have $u = v$, but that means from the above that $(x, u) \in f \wedge (x', u) \in f$, which as f is injective proves

$$x = x'$$

2. Let $z \in C$ then as g is surjective there $\exists y \in B$ such that $(y, z) \in g$. As f is surjective there exists a $x \in A$ such that $(x, y) \in f$. But then $(x, z) \in g \circ f$ proving that $g \circ f$ is surjective.
3. If $f: A \rightarrow B$ and $g: B \rightarrow A$ are bijections then these two functions are injective and surjective. Using (1) and (2) proves that $g \circ f: A \rightarrow C$ is injective and surjective and thus by definition bijective.

4. By (3) $g\circ f$ is a bijection, so by [theorem: 2.64] we have that

$$
\begin{aligned}
(g\circ f)^{-1}\circ(g\circ f)=\mathrm{Id}_A &\underset{\text{[associativity: 2.18]}}{\Rightarrow} ((g\circ f)^{-1}\circ g)\circ f=\mathrm{Id}_A\\
&\Rightarrow (((g\circ f)^{-1}\circ g)\circ f)\circ f^{-1}=\mathrm{Id}_A\circ f^{-1}\\
&\underset{\text{[proposition: 2.43]}}{\Rightarrow} (((g\circ f)^{-1}\circ g)\circ f)\circ f^{-1}=f^{-1}\\
&\underset{\text{[associativity: 2.18]}}{\Rightarrow} ((g\circ f)^{-1}\circ g)\circ(f\circ f^{-1})=f^{-1}\\
&\underset{\text{[theorem: 2.64]}}{\Rightarrow} ((g\circ f)^{-1}\circ g)\circ\mathrm{Id}_B=f^{-1}\\
&\underset{\text{[proposition: 2.43]}}{\Rightarrow} (g\circ f)^{-1}\circ g=f^{-1}\\
&\Rightarrow ((g\circ f)^{-1}\circ g)\circ g^{-1}=f^{-1}\circ g^{-1}\\
&\underset{\text{[associativity: 2.18]}}{\Rightarrow} (g\circ f^{-1})\circ(g\circ g^{-1})=f^{-1}\circ g^{-1}\\
&\underset{\text{[theorem: 2.64]}}{\Rightarrow} (g\circ f)^{-1}\circ\mathrm{Id}_A=f^{-1}\circ g^{-1}\\
&\underset{\text{[proposition: 2.43]}}{\Rightarrow} (g\circ f)^{-1}=f^{-1}\circ g^{-1}
\end{aligned}
$$

□

The following is a example of a bijection between a class and the class of functions in this set.

Theorem 2.70. *Let A be a class then there exists a bijection between A and $A^{\{0\}}$*

Proof. Given $x\in A$ define the function $f_x:\{0\}\rightarrow\{x\}$ where $f_x=\{(0,x)\}$ [see [example: 2.61] to prove that this is a function (even a bijection)]. So $f_x\in\{x\}^{\{0\}}$, which as $\{x\}\subseteq A$ proves by [theorem: 2.29] that $f_x\in A^{\{0\}}$. Define now $f=\{z|z=(x,f_x)\text{ where }x\in A\}$. If $(x,y)\in f$ we have $x\in A$ and thus $y=f_x\in A^{\{0\}}$ hence $(x,y)\in A\times A^{\{0\}}$. Also if $(x,y),(x,y')\in A$ then $y=f_x$ and $y'=f_x$ so that $y=y'$. Further for every $x\in A$ we have by the definition of f that $(x,f_x)\in f$. So we conclude that

$$f: A\rightarrow A^{\{0\}}\text{ is a function}$$

Assume now that $(x,y),(x',y)\in f$ then $f_x=y=f_{x'}$, so that $\{(0,x)\}=\{(0,x')\}$, hence $(0,x)=(0,x')$, from which it follows that $x=x'$. this proves that

$$f: A\rightarrow A^{\{0\}}\text{ is a injective function}$$

If $y\in A^{\{0\}}$ then $y:\{0\}\rightarrow A$ is a function, hence $0\in\{0\}=\mathrm{dom}(y)$, so there exists a z such that $(0,z)\in y\subseteq\{0\}\times A$ proving that $z\in A$. Hence

$$\{(0,z)\}\subseteq y\wedge z\in A \tag{2.18}$$

If $(u,v)\in y\subseteq\{0\}\times A$ then $u=0$ so that $(0,u)\in y$, which, as $(0,z)\in y$ and y is a function, proves that $u=z$ or $(u,v)=(0,z)\in\{(0,z)\}$. So $y\subseteq\{(0,z)\}$ which combined with [eq: 2.18] proves that $\{(0,z)\}=y$. As $f_z=\{(0,z)\}=y$ we have that $(z,y)\in f$ which proves that

$$f\text{ is a surjection}$$

□

Theorem 2.71. *If A is a class then there is a bijection between $\mathcal{P}(A)$ and $\{0,1\}^A$ where $0=\varnothing$ and $1=\{\varnothing\}$ are different elements.*

Proof. Define $\gamma:\mathcal{P}(A)\rightarrow\{0,1\}^A$ by $\gamma=\{z|z=(B,\mathcal{X}_{A,B})\text{ where }B\in\mathcal{P}(A)\}$ where $\mathcal{X}_{A,B}=(B\times\{1\})\bigcup((A\setminus B)\times\{0\})$ is the graph of the Characteristic function [example: 2.41]. If $(B,f)\in\gamma$ then $B\in\mathcal{P}(A)$ and $f=\mathcal{X}_{A,B}$, as $B\in\mathcal{P}(A)\Rightarrow B\subseteq A$ it follow using [example: 2.41] that $\mathcal{X}_{A,B}: A\rightarrow\{0,1\}$ is a function. So $(B,f)\in\{0,1\}^A$ giving

$$\gamma\subseteq\mathcal{P}(A)\times(\{0,1\}^A)$$

If $(B,f),(B,g)\in\gamma$ then $f=\mathcal{X}_{A,B}$ and $g=\mathcal{X}_{A,B}$ so that $f=g$, also by the definition of γ we have that $\mathrm{dom}(\gamma)=\mathcal{P}(A)$, hence

$$\gamma:\mathcal{P}(A)\rightarrow\{0,1\}^A\text{ is a function}$$

If $(B, f), (B', f) \in \gamma$ then $\mathcal{X}_{A,B} = \mathcal{X}_{A,B'}$ so that

$$\begin{array}{rcl} x \in B & \Leftrightarrow & \mathcal{X}_{A,B}(x) = 1 \\ & \underset{\mathcal{X}_{A,B} = \mathcal{X}_{A,B'}}{\Leftrightarrow} & \mathcal{X}_{A,B'}(x) = 1 \\ & \Leftrightarrow & x \in B' \end{array}$$

proving that $B = B'$. Hence

$$\gamma: \mathcal{P}(A) \rightarrow \{0,1\}^A \text{ is injective}$$

Let $f \in \{0,1\}^A$, define $B = \{x \in A | (x,1) \in f\} \subseteq A$, then $B \in \mathcal{P}(A)$.

If $(x, y) \in f$ then we have for x either:

$x \in B$. Then $(x,1) \in f$ and as $(x, y) \in f$ we have that $y = 1$ so that $(x, y) = (x, 1) \in \mathcal{X}_{A,B}$

$x \notin B$. Then $(x,0) \in f$ and as $(x, y) \in f$ we have that $y = 0$ so that $(x, y) = (x, 0) \in \mathcal{X}_{A,B}$ [as $x \in A \setminus B$]

proving that

$$f \subseteq \mathcal{X}_{A,B} \tag{2.19}$$

If $(x, y) \in \mathcal{X}_{A,B}$ then we have for x either:

$x \in B$. Then as $(x,1) \in \mathcal{X}_{A,B}$ we must have that $y = 1$, using the definition of B we have also $(x, 1) \in f \Rightarrow (x, y) \in f$

$x \notin B$. Then $x \in A \setminus B$ so that $(x, 0) \in \mathcal{X}_{A,B}$ hence we must have that $y = 0$. As $(x, 0) \in f$ [if $(x, 1) \in f$ then $x \in B$ a contradiction] it follows that $(x, y) = (x, 0) \in f$

proving that $\mathcal{X}_{A,B} \subseteq f$, which combined with 2.19 gives

$$\mathcal{X}_{A,B} = f \tag{2.20}$$

So given $f \in \{0,1\}^A$ we have found a $B \in \mathcal{P}(A)$ such that $\mathcal{X}_{A,B} \underset{\text{[eq: 2.20]}}{=} f$, hence $(B, f) \in \gamma$ proving that

$$\gamma: \mathcal{P}(A) \rightarrow \{0,1\}^A \text{ is a surjective}$$ □

2.2.4 Restriction of a Function/Partial Function

Sometimes we only want to work with functions whose graphs satisfies certain conditions. It could be that the graph of a function does not satisfies these, but that the restriction of this graph to a sub-class satisfies the conditions. For example, the function $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = \left\{\begin{smallmatrix} 1 \text{ if } x < 1 \\ 0 \text{ if } 1 \leqslant x \end{smallmatrix}\right.$ is not continuous, as it is discontinuous at 1. However restricting this function to $\mathbb{R} \setminus \{1\}$ produces a continuous function. This is the idea of the next definition

Definition 2.72. *Let $f: A \rightarrow B$ be a partial function and $C \subseteq A$ a sub-class of A then the restriction of f to C noted by $f_{|C}$ is defined by*

$$f_{|C} = \{z | z = (x, y) \in f \wedge x \in C\} = f \bigcap (C \times B)$$

which defines the partial function

$$f_{|C}: C \rightarrow B$$

Proof. We must of course proof that $\{z | z = (x, y) \in f \wedge x \in C\}$ and that $f_{|C}: C \rightarrow B$ is indeed a partial function. If $(x, y) \in \{z | z = (x, y) \in f \wedge x \in C\}$ then $(x, y) \in f \subseteq A \times B \Rightarrow y \in B$ and $x \in C$, so that $(x, y) \in f \wedge (x, y) \in C \times B$, hence $(x, y) \in f \bigcap (C \times B)$. If $(x, y) \in f \bigcap (C \times B)$ then $(x, y) \in f \wedge (x, y) \in C \times B \Rightarrow x \in C$, proving that $(x, y) \in \{z | z = (x, y) \in f \wedge x \in C\}$. So we have that

$$f_{|C} = \{z | z = (x, y) \in f \wedge x \in C\} = f \bigcap (C \times B)$$

From the above it follows, using [theorem: 1.25], that

$$f_{|C} \subseteq C \times B$$

Finally, if $(x,y),(x,y') \in f_{|C}$ then $(x,y),(x,y') \in f$ so that $y = y'$. Hence we have that $f_{|C}: C \rightarrow B$ is a partial function. ☐

Theorem 2.73. *Let $f: A \rightarrow C$ and $g: B \rightarrow C$ be two partial functions such that $A \bigcap B = \varnothing$ then*

1. *$f \bigcup g: A \bigcup B \rightarrow C$ is a partial function*
2. *$f = (f \bigcup g)_{|A}$ and $g = (f \bigcup g)_{|B}$*
3. *$\mathrm{dom}(f \bigcup g) = \mathrm{dom}(f) \bigcup \mathrm{dom}(g)$*
4. *If $f: A \rightarrow C$ and $g: B \rightarrow C$ are functions then $f \bigcup g: A \bigcup B \rightarrow C$ are functions*

Proof.

1. As $f: A \rightarrow C$ and $g: B \rightarrow C$ are functions we have that $f \subseteq A \times C$ and $g \subseteq B \times C$ so that by [theorem: 1.25]

$$f \bigcup g \subseteq (A \times C) \bigcup (B \times C) \underset{\text{[theorem: 1.49]}}{=} \left(A \bigcup B\right) \times C$$

Let $(x,y),(x,y') \in f \bigcup g$. Assume that $y \neq y'$ then we can not have that $(x,y),(x,y') \in f$ for then, as f is a function, we would have $y = y'$, likewise we can not have that (x,y), $(x,y') \in g$, for then, as g is a function, we would have that $y = y'$. So we must that either $(x,y) \in f \wedge (x,y') \in g$ or $(x,y) \in g \wedge (x,y') \in f$, but then we would have $x \in A \bigcap B$ which contradicts $A \bigcap B = \varnothing$. So we must have that $y = y'$. Summarized

$$\text{If } (x,y),(x,y) \in f \bigcup g \text{ then we have } y = y'$$

2. As $f \subseteq A \times C$ we have by [theorem :1.25] that

$$f \bigcap (B \times C) \subseteq (A \times C) \bigcap (B \times C) \underset{\text{[theorem: 1.49]}}{=} \left(A \bigcap B\right) \times C = \varnothing \times C \underset{\text{[theorem: 1.47}}{=} \varnothing$$

proving using [theorem: 1.18] that

$$f \bigcap (B \times C) = \varnothing \tag{2.21}$$

As $g \subseteq B \times C$ we have by [theorem :1.25] that

$$g \bigcap (A \times C) \subseteq (B \times C) \bigcap (A \times C) \underset{\text{[theorem: 1.49]}}{=} \left(A \bigcap B\right) \times C = \varnothing \times C \underset{\text{[theorem: 1.47}}{=} \varnothing$$

proving using [theorem: 1.18 that

$$g \bigcap (A \times C) = \varnothing \tag{2.22}$$

Further we have

$$\begin{array}{lcl}
\left(f \bigcup g\right)_{|A} & = & \left(f \bigcup g\right) \bigcap (A \times C) \\
 & \underset{\text{[theorem: 1.30}}{=} & \left(f \bigcap (A \times C)\right) \bigcup \left(g \bigcap (A \times C)\right) \\
 & \underset{\text{[eq: 2.22]}}{=} & \left(f \bigcap (A \times C)\right) \bigcup \varnothing \\
 & \underset{\text{[theorem: 1.32]}}{=} & f \bigcap (A \times C) \\
 & \underset{f \subseteq A \times C \text{snd [theorem:1.26]}}{=} & f \\
\left(f \bigcup g\right)_{|B} & = & \left(f \bigcup g\right) \bigcap (B \times C) \\
 & \underset{\text{[theorem: 1.30}}{=} & \left(f \bigcap (B \times C)\right) \bigcup \left(g \bigcap (B \times C)\right) \\
 & \underset{\text{[eq: 2.21]}}{=} & \varnothing \bigcup \left(\bigcap (B \times C)\right) \\
 & \underset{\text{[theorem: 1.32]}}{=} & g \bigcap (B \times C) \\
 & \underset{g \subseteq B \times C \text{snd [theorem:1.26]}}{=} & g
\end{array}$$

3.

$$\begin{aligned} x \in \operatorname{dom}\left(f \bigcup g\right) &\Leftrightarrow \exists y \text{ such that } (x, y) \in f \bigcup g \\ &\Leftrightarrow \exists y \text{ such that } (x, y) \in f \vee (x, y) \in g \\ &\Rightarrow x \in \operatorname{dom}(f) \vee x \in \operatorname{dom}(g) \\ &\Rightarrow x \in \operatorname{dom}(f) \bigcup \operatorname{dom}(g) \\ x \in \operatorname{dom}(f) \bigcup \operatorname{dom}(g) &\Rightarrow x \in \operatorname{dom}(f) \vee x \in \operatorname{dom}(g) \\ &\Rightarrow (\exists y \text{ such that } (x, y) \in f) \vee (\exists y' \text{ such that } (x, y) \in g) \\ &\Rightarrow \left(\exists y \text{ such that } (x, y) \in f \bigcup g\right) \vee \left(\exists y' \text{ such that } (x, y) \in f \bigcup g\right) \\ &\Rightarrow x \in \operatorname{dom}\left(f \bigcup g\right) \end{aligned}$$

so

$$\operatorname{dom}\left(f \bigcup g\right) = \operatorname{dom}(f) \bigcup \operatorname{dom}(g)$$

4. As $f: A \rightarrow C$ and $g: B \rightarrow C$ are functions we have that $A = \operatorname{dom}(f)$, $B = \operatorname{dom}(g)$. So that

$$\operatorname{dom}\left(f \bigcup g\right) \underset{(3)}{=} \operatorname{dom}(f) \bigcup \operatorname{dom}(g) = A \bigcup B$$

proving that

$$f \bigcup g: A \bigcup B \rightarrow C \text{ is a function}$$ □

Corollary 2.74. *Let $f: A \rightarrow B$ and $g: C \rightarrow D$ be functions such that $A \bigcap C = \varnothing$ then*

$$f \bigcup g: A \bigcup C \rightarrow B \bigcup D$$

is a function.

Proof. Using [theorem: 2.28] we have that $f: A \rightarrow B \bigcup D$ and $g: C \rightarrow B \bigcup D$ are functions. Applying then the previous theorem [theorem: 2.73] proves that $f \bigcup g: A \bigcup C \rightarrow B \bigcup D$ is a function. □

Corollary 2.75. *Let $f: A \rightarrow B$ and $g: C \rightarrow D$ be bijections with $A \bigcap C = \varnothing$ and $B \bigcap D = \varnothing$ then*

$$f \bigcup g: A \bigcup C \rightarrow B \bigcup D$$

is a bijection.

Proof. Using the previous theorem [theorem: 2.74] we have that $f \bigcup g: A \bigcup C \rightarrow B \bigcup D$ is a function. Now we have:

injectivity. If $(x, y), (x', y) \in f \bigcup g \subseteq (A \bigcup C) \times (B \bigcup D)$ we have the following possibilities for y:

- **$y \in B$.** As $f \subseteq A \times B$ and $g \subseteq C \times D$ we can not have $(x, y), (x', y) \in g$ [for then $y \in D \Rightarrow y \in B \bigcap D = \varnothing$], as g is injective we have $x = x'$.
- **$y \in D$.** As $f \subseteq A \times B$ and $g \subseteq C \times D$ we can not have $(x, y), (x', y) \in f$ [for then $y \in B \Rightarrow y \in B \bigcap D = \varnothing$], as f is injective we have $x = x'$.

so in all cases we have $x = x'$ proving injectivity of $f \bigcup g: A \bigcup C \rightarrow B \bigcup D$.

surjectivity. If $y \in B \bigcup D$ then we have either:

- **$y \in B$.** Then as f is surjective there exist a $x \in A \subseteq A \bigcup C$ such that $(x, y) \in f \subseteq f \bigcup g$.
- **$y \in D$.** Then as g is surjective there exist a $x \in C \subseteq A \bigcup C$ such that $(x, y) \in g \subseteq f \bigcup g$.

proving that in all cases there exist a $x \in A \bigcup C$ such that $(x, y) \in f \bigcup g$. □

Corollary 2.76. *Let $f: A \rightarrow B$ be a function a, b elements such that $a \notin A$ then*

$$g: A \bigcup \{a\} \rightarrow B \bigcup \{b\} \text{ defined by } g = \{(a, b)\} \bigcup f$$

is a function.

Note 2.77. *A alternative definition of g is* $g(x) = \left\{ \begin{smallmatrix} b \text{ if } x = a \\ f(x) \text{ if } x \in A \end{smallmatrix} \right.$

Proof. Using [example: 2.40] we have that $C_b: \{a\} \rightarrow \{b\}$ where $C_b = \{(x, b) | x \in \{a\}\} = \{(a, b)\}$ is a function. As $A \bigcap \{a\}$ we can use the previous corollary [corollary: 2.74] so that

$$h: A \bigcup \{a\} \rightarrow B \bigcup \{b\} \text{ where } h = \{(a, b)\} \bigcup f \text{ is a function} \qquad \square$$

Theorem 2.78. *Let $f: A \rightarrow B$ be a partial function and $C \subseteq A$ a sub-class of A then we have:*

1. $\mathrm{dom}(f_{|C}) = C \bigcap \mathrm{dom}(f)$
2. $\mathrm{range}(f_{|C}) = f(C)$
3. *If $D \subseteq C$ then $f_{|C}(D) = f(D)$*
4. *If $E \subseteq B$ then $(f_{|C})^{-1}(E) = C \bigcap f^{-1}(E)$*
5. *If $f: A \rightarrow B$ is injective then $f_{|C}: C \rightarrow B$ is injective*

Proof.

1. If $x \in \mathrm{dom}(f_{|C})$ then there exists a y such that $(x, y) \in f_{|C}$, hence $x \in C$ and $(x, y) \in f$ or $x \in C$ and $x \in \mathrm{dom}(f)$, so that $x \in C \bigcap \mathrm{dom}(f)$. Hence

   $$\mathrm{dom}(f_{|C}) \subseteq C \bigcap \mathrm{dom}(f) \tag{2.23}$$

   Further if $x \in C \bigcap \mathrm{dom}(f)$ then $x \in C$ and $x \in \mathrm{dom}(f)$, so there exists a y such that $(x, y) \in f$, hence $(x, y) \in f_{|C}$ or $x \in \mathrm{dom}(f_{|C})$. So $C \bigcap \mathrm{dom}(f) \subseteq \mathrm{dom}(f_{|C})$ which together with [eq: 2.23] gives

   $$\mathrm{dom}(f_{|C}) = C \bigcap \mathrm{dom}(f)$$

2. If $y \in \mathrm{range}(f_{|C})$ then $\exists x$ such that $(x, y) \in f_{|C}$, hence $(x, y) \in f$ and $x \in C$, so that $y \in f(C)$. On the other hand if $y \in f(C)$ there exists a $x \in C$ such that $(x, y) \in f$, hence $(x, y) \in f_{|C}$ so that $y \in \mathrm{range}(f_{|C})$. Hence using the Axiom of Extent [axiom: 1.5] we have

   $$\mathrm{range}(f_{|C}) = f(C)$$

3. If $y \in f_{|C}(D)$ then $\exists x \in D$ such that $(x, y) \in f_{|C}$, hence $(x, y) \in f$ so that $y \in f(D)$. On the other hand if $y \in f(D)$ then $\exists x \in D$ such that $(x, y) \in f$, which as $x \in D \subseteq C \Rightarrow x \in C$ proves that $(x, y) \in f_{|C}$, so $y \in f_{|C}(D)$. Hence using the Axiom of Extent [axiom: 1.5] we have

   $$f_{|C}(D) = f(D)$$

4. If $x \in (f_{|C})^{-1}(E)$ then there exist a $y \in E$ such that $(x, y) \in f_{|C}$, hence $x \in C$ and $(x, y) \in f \Rightarrow x \in f^{-1}(E)$, so that $x \in C \bigcap f^{-1}(E)$. Further if $x \in C \bigcap f^{-1}(E)$ then $x \in C$ and $x \in f^{-1}(E)$, so there exist a $y \in E$ such that $(x, y) \in f \underset{x \in C}{\Rightarrow} (x, y) \in f_{|C}$, hence $x \in (f_{|C})^{-1}(E)$. Hence using the Axiom of Extent [axiom: 1.5] we have

   $$(f_{|C})^{-1}(E) = C \bigcap f^{-1}(E)$$

5. If $(x, y), (x', y) \in f_{|C}$ then as $f_{|C} \subseteq f$ we have $(x, y), (x', y) \in f$ which as f is injective proves $y = y'$ $\square$

Theorem 2.79. *Let $f: A \rightarrow B$ be a partial function then $f_{|\mathrm{dom}(f)} = f$*

Proof. If $(x, y) \in f$ then by definition $x \in \mathrm{dom}(f)$ hence $(x, y) \in f_{|\mathrm{dom}(f)}$, further if $(x, y) \in f_{|\mathrm{dom}(f)}$ then $(x, y) \in f$ and $x \in \mathrm{dom}(f)$, so evidently $(x, y) \in f$. Hence using the Axiom of Extent [axiom: 1.5] we have

$$f_{|\mathrm{dom}(f)} = f \qquad \square$$

Theorem 2.80. *Let $f: A \rightarrow B$ be a injective partial function and $C \subseteq A$ then $(f^{-1})_{|f(C)} = (f_{|C})^{-1}$*

Proof. Let $(x, y) \in (f^{-1})_{|f(C)}$ then $x \in f(C)$ and $(x, y) \in f^{-1} \Rightarrow (y, x) \in f$, as $x \in f(C)$ there exists a $z \in C$ such that $(z, x) \in f$. As f is injective we have that $z = y$, proving that $y \in C$, which as $(y, x) \in f$ gives $(y, x) \in f_{|C}$ so that $(x, y) \in (f_{|C})^{-1}$. Hence

$$(f^{-1})_{|f(C)} \subseteq (f_{|C})^{-1} \tag{2.24}$$

If $(x, y) \in (f_{|C})^{-1}$ then $(y, x) \in f_{|C}$ so that $y \in C$ and $(y, x) \in f$. Hence $x \in f(C)$ and as $(y, x) \in f$ gives $(x, y) \in f^{-1}$ we have $(x, y) \in (f^{-1})_{|f(C)}$. This proves that $(f_{|C})^{-1} \subseteq (f^{-1})_{|f(C)}$, combing this with [eq: 2.24] gives:

$$(f^{-1})_{f(C)} = (f_{|C})^{-1}$$ □

Theorem 2.81. *Let $f: A \rightarrow B$ and $g: B \rightarrow C$ be partial functions and $C \subseteq A$ then*

$$(g \circ f)_{|C} = g_{|f(C)} \circ f_{|C}$$

Proof. Let $(x, z) \in (f \circ g)_{|C}$ then $(x, z) \in f \circ g$ and $x \in C$. Hence $\exists y$ such that $(x, y) \in f \wedge (y, z) \in g$, as $x \in C$ $(x, y) \in f_{|C}$. From $x \in C$ and $(x, y) \in f$ it follows also that $y \in f(C)$, hence as $(y, z) \in g$ we have that $(y, z) \in g_{|f(C)}$. From $(x, y) \in f_{|C}$ and $(y, z) \in g_{|f(C)}$ it follows that $(x, z) \in g_{|f(C)} \circ f_{|C}$ so that

$$(g \circ f)_{|C} \subseteq g_{|f(C)} \circ f_{|C} \tag{2.25}$$

If $(x, z) \in g_{|f(C)} \circ f_{|C}$ then there exists a y such that $(x, y) \in f_{|C}$ and $(y, z) \in g_{|f(C)}$, so $x \in C$, $(x, y) \in f$, $y \in f(C)$ and $(y, z) \in g$. Hence $x \in C$ and $(x, z) \in g \circ f$ proving that $(x, z) \in (g \circ f)_{|C}$. So $g_{|f(C)} \circ f_{|C} \subseteq (g \circ f)_{|C}$ which combined with [eq: 2.25] gives

$$(g \circ f)_{|C} = g_{|f(C)} \circ g_{|C}$$ □

Theorem 2.82. *Let $f: A \rightarrow B$ and $C \subseteq A$ a sub-class of A then $f_{|C}: C \rightarrow B$ is a function.*

Proof. Using [definition: 2.72] we have that $f_{|C}: C \rightarrow B$ is a partial function, as by [theorem: 2.78] $\mathrm{dom}(f_{|C}) = C \bigcap \mathrm{dom}(f) \underset{f \text{ is a function}}{=} C \bigcap A \underset{C \subseteq A}{=} C$, it follows that $f_{|C}: C \rightarrow B$ is a function. □

The following theorem will be used for manifolds later

Theorem 2.83. *Let $f: A \rightarrow B$ and $g: C \rightarrow B$ be injections then we have*

1. *$f: A \rightarrow f(A)$ and $g: C \rightarrow f(C)$ are bijections*
2. *$\mathrm{dom}(f \circ g^{-1}) = g(A \bigcap C)$*
3. *$f \circ g^{-1} = (f \circ g^{-1})_{|g(A \bigcap C)} = f_{|A \bigcap C} \circ (g^{-1})_{|g(A \bigcap C)} = f_{|(A \bigcap C)} \circ (g_{|A \bigcap C})^{-1}$*

Proof.

1. This follows from [proposition: 2.62]
2. If $z \in \mathrm{dom}(f \circ g^{-1})$ then $\exists x$ such that $(z, x) \in f \circ g^{-1}$, hence $\exists y$ such that $(z, y) \in g^{-1}$ and $(y, z) \in f$, from which it follows that $(y, z) \in g$ and $(y, z) \in f$. As $g \subseteq C \times B$ and $f \subseteq A \times B$ it follows that $y \in A$ and $y \in C$ so that $y \in A \bigcap C$, as $(y, z) \in g$ we have $z \in g(A \bigcap C)$. This proves

$$\mathrm{dom}(g \circ f^{-1}) \subseteq g\left(A \bigcap C\right) \tag{2.26}$$

If $z \in g(A \bigcap C)$ then $\exists y \in A \bigcap C$ such that $(y, z) \in g$, hence $(z, y) \in g^{-1}$. As f is a function we have that $A = \mathrm{dom}(f)$, hence as $y \in A \bigcap C \Rightarrow y \in A$, there exists a x such that $(y, x) \in f$. As $(z, y) \in g^{-1}$ we have $(z, x) \in f \circ g^{-1}$ proving that $z \in \mathrm{dom}(f \circ g^{-1})$. Hence $g(A \bigcap C) \subseteq \mathrm{dom}(g \circ f^{-1})$ which combined with [eq: 2.26].

$$\mathrm{dom}(g \circ f^{-1}) = g\left(A \bigcap C\right)$$

3. We have

$$\begin{aligned}(f\circ g^{-1}) &\underset{[\text{theorem: } 2.79]}{=} (f\circ g^{-1})_{\mathrm{dom}(f\circ g^{-1})}\\ &\underset{(1)}{=} (f\circ g^{-1})_{g(A\bigcap C)}\\ &\underset{[\text{theorem: } 2.81]}{=} f_{|g^{-1}(g(A\bigcap C))}\circ (g^{-1})_{g(A\bigcap C)}\\ &\underset{g\text{ is injective and [theorem: } 2.51]}{=} f_{|A\bigcap C}\circ (g^{-1})_{|g(A\bigcap C)}\\ &\underset{[\text{theorem: } 2.80]}{=} f_{|A\bigcap C}\circ (g_{|A\bigcap C})^{-1}\end{aligned}$$

□

2.2.5 Set operations and (Partial) Functions

Theorem 2.84. *Let $f: A \rightarrow B$ be a function then we have*

1. *If $C, D \subseteq A$ with $C \subseteq D$ then $f(C) \subseteq f(D)$*
2. *If $C, D \subseteq B$ with $C \subseteq D$ then $f^{-1}(C) \subseteq f^{-1}(D)$*
3. *If $C, D \subseteq B$ then $f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D)$*
4. *If $D \subseteq B$ then $f^{-1}(B \setminus D) = A \setminus f^{-1}(D)$*
5. *If $C, D \subseteq A$ then $f(C) \setminus f(D) \subseteq f(C \setminus D)$*
6. *If $C, D \subseteq A$ and f is **injective** then $f(C) \setminus f(D) = f(C \setminus D)$*

Proof.

1. Let $y \in f(C)$ then there exist a $x \in C$ such that $(x, y) \in f$, as $C \subseteq D$ we have $x \in D$ so that $y \in f(D)$
2. If $x \in f^{-1}(C)$ there exists a $y \in C$ such that $(x, y) \in f$, as $C \subseteq D$ then $y \in D$ so that $x \in f^{-1}(D)$
3. If $x \in f^{-1}(C \setminus D)$ then $\exists y \in C \setminus D$ such that $(x, y) \in f$. As $y \in C \setminus D$ we have that $y \in C$ and $y \notin D$, from $y \in C$ it follows that $x \in f^{-1}(C)$. Assume that also $x \in f^{-1}(D)$ then $\exists y' \in D$ such that $(x, y') \in f$ which, as f is a function and $(x, y) \in f$, proves that $y = y'$, hence $y \in D$ contradicting $y \notin D$, so we must have $x \notin f^{-1}(D)$, hence $x \in f(C) \setminus f(D)$ proving

$$f^{-1}(C \setminus D) \subseteq f^{-1}(C) \setminus f^{-1}(D) \tag{2.27}$$

   If $x \in f^{-1}(C) \setminus f^{-1}(D)$ then $x \in f^{-1}(C)$ and $x \notin f^{-1}(D)$. As $x \in f^{-1}(C)$ there exists a $y \in C$ such that $(x, y) \in f$. Assume that $y \in D$, then as $(x, y) \in f$ we have $x \in f^{-1}(D)$ contradicting $x \notin f^{-1}(D)$, so we must have $y \notin D$. Hence $y \in C \setminus D$ which proves that $x \in f^{-1}(C \setminus D)$ or $f^{-1}(C) \setminus f^{-1}(D) \subseteq f^{-1}(C \setminus D)$. Combining this with [eq: 2.27] proves

$$f^{-1}(C \setminus D) = f^{-1}(C) \setminus f^{-1}(D)$$

4. As $D \subseteq B \subseteq B$ we have by (3) that

$$\begin{aligned}f^{-1}(B \setminus D) &= f^{-1}(B) \setminus f^{-1}(D)\\ &\underset{[\text{theorem: } 2.44]}{=} A \setminus f^{-1}(D)\end{aligned}$$

5. If $y \in f(C) \setminus f(D)$ then $y \in f(C)$ and $y \notin f(D)$. From $y \in f(C)$ it follows that $\exists x \in C$ such that $(x, y) \in f$. Assume that $x \in D$ then as $(x, y) \in f$ we have $y \in f(D)$ contradicting $y \notin f(D)$, so we must have $x \notin D$, proving that $x \in C \setminus D$. Hence $y \in f(C \setminus D)$ or

$$f(C) \setminus f(D) \subseteq f(C \setminus D)$$

6. If $y \in f(C \setminus D)$ then $\exists x \in C \setminus D$ such that $x \in C$, $x \notin D$ and $(x, y) \in f$. From $x \in C$ it follows that $y \in f(C)$. Assume that $y \in f(D)$ then there exist a $x' \in D$ such that $(x', y) \in f$, as f is **injective** we have $x = x'$ so that $x \in D$ contradicting $x \notin D$, hence $y \notin f(D)$. This proves that $y \in f(C) \setminus f(D)$ or $f(C \setminus D) \subseteq f(C) \setminus f(D)$ which combined with (3) gives

$$f(C) \setminus f(D) = f(C \setminus D)$$

□

Theorem 2.85. *If $f: A \rightarrow B$ is a function, $E, F \subseteq A$ and $C, D \subseteq B$ then we have*

1. $f(E \bigcup F) = f(E) \bigcup f(F)$
2. $f^{-1}(C \bigcup D) = f^{-1}(C) \bigcup f^{-1}()$
3. $f(E \bigcap F) \subseteq f(E) \bigcap f(F)$
4. *If f is injective then* $f(E \bigcap F) = f(E) \bigcap f(F)$
5. $f^{-1}(C \bigcap D) = f^{-1}(C) \bigcap f^{-1}(D)$

Proof.

1. Let $y \in f(E \bigcup F)$ then there exist a $x \in E \bigcup F$ with $(x, y) \in f$. So $x \in E$ proving that $y \in f(E)$ or $x \in F$ proving $y \in f(F)$. So it follows that $y \in f(E) \bigcup f(F)$ or

$$f\left(E \bigcup F\right) \subseteq f(E) \bigcup f(F) \tag{2.28}$$

If $y \in f(E) \bigcup f(F)$ then we have the following possibilities

$y \in f(E)$. Then $\exists x \in E$ such that $(x, y) \in f$. As by the definition of a union $x \in E \bigcup F$, it follows that $y \in f(E \bigcup F)$

$y \in f(F)$. Then $\exists x \in F$ such that $(x, y) \in f$. As by the definition of a union $x \in E \bigcup F$, it follows that $y \in f(E \bigcup F)$

So in all cases we have $y \in f(E \bigcup F)$. Hence $f(E) \bigcup f(F) \subseteq f(E \bigcup F)$ which combined with [eq: 2.28] proves

$$f\left(E \bigcup F\right) = f(E) \bigcup f(F)$$

2. If $x \in f^{-1}(C \bigcup D)$ there exists a $y \in C \bigcup D$ such that $(x, y) \in f$. From $y \in C \bigcup D$ we have $y \in C$ hence $x \in f^{-1}(C)$ or $y \in D$ hence $x \in f^{-1}(D)$. So $x \in f^{-1}(C) \bigcup f^{-1}(D)$ proving

$$f^{-1}\left(C \bigcup D\right) \subseteq f^{-1}(C) \bigcup f^{-1}(D) \tag{2.29}$$

If $x \in f^{-1}(C) \bigcup f^{-1}(D)$ then we have the following possibilities to consider:

$x \in f^{-1}(C)$. Then $\exists y \in C$ such that $(x, y) \in f$. As by the definition of a union $y \in C \bigcup D$ it follows that $x \in f^{-1}(C \bigcup D)$

$x \in f^{-1}(D)$. Then $\exists y \in D$ such that $(x, y) \in f$. As by the definition of a union $y \in C \bigcup D$ it follows that $x \in f^{-1}(C \bigcup D)$

So in all cases we have $x \in f^{-1}(C \bigcup D)$, proving $f^{-1}(C) \bigcup f^{-1}(D) \subseteq f^{-1}(C \bigcup D)$ which combined with [eq 2.29] proves

$$f^{-1}\left(C \bigcup D\right) = f^{-1}(C) \bigcup f^{-1}(D)$$

3. If $y \in f(E \bigcap F)$ then $\exists x \in E \bigcap F$ such that $(x, y) \in f$. From $x \in E \bigcap F$ we have that $x \in E$ hence $y \in f(E)$ and $x \in F$, so that $y \in f(F)$. Hence $y \in f(E) \bigcap f(F)$ or

$$f\left(E \bigcap F\right) \subseteq f(E) \bigcap f(F)$$

4. Using (3) we have that

$$f\left(E \bigcap F\right) \subseteq f(E) \bigcap f(F) \tag{2.30}$$

Let $y \in f(E) \bigcap f(F)$ then we have $y \in f(E)$ so that $\exists x \in E$ such that $(x, y) \in f$ and $y \in f(F)$ so that $\exists x' \in F$ such that $(x', y) \in f$. As f is injective and $(x, y), (x', y) \in f$ we have $x = x'$ so that $x \in E \bigcap F$, proving that $f(E) \bigcap f(F) \subseteq f(E \bigcap F)$. Combining this result with [eq: 2.30] gives

$$f\left(E \bigcap F\right) = f(E) \bigcap f(F)$$

5. If $x \in f^{-1}(C \bigcap D)$ then $\exists y \in C \bigcap D$ such that $y \in C$, so that $x \in f^{-1}(C)$ and $y \in D$, so that $x \in f^{-1}(D)$. Hence $x \in f^{-1}(C) \bigcap f^{-1}(D)$ proving

$$f^{-1}\left(C \bigcap D\right) \subseteq f^{-1}(C) \bigcap f^{-1}(D) \tag{2.31}$$

If $x \in f^{-1}(C) \bigcap f^{-1}(D)$ then $x \in f^{-1}(C)$ so there exists a $y \in C$ such that $(x, y) \in f$ and $x \in f^{-1}(D)$ so $\exists y' \in D$ such that $(x, y') \in f$. As f is a function $y = y'$ proving $y \in C \bigcap D$, hence $x \in f^{-1}(C \bigcap D)$. So $f^{-1}(C) \bigcap f^{-1}(D) \subseteq f^{-1}(C \bigcap D)$, combining this with [eq: 2.31] gives

$$f^{-1}\left(C \bigcap D\right) = f^{-1}(C) \bigcap f^{-1}(D) \qquad \square$$

Up to now we define a function $f: A \rightarrow B$ by specifying what the classes f, A, B are. However in many cases we have a parameterized expression [based on function calls and operators) to define f. Then we have the following

Proposition 2.86. *Let A, B be classes and suppose that there exists a parameterized expression $F(x)$ that calculates a **unique** value for **every** $x \in A$ then we can define the function $f: A \rightarrow B$ by $f = \{z | z = (x, F(x)) \wedge x \in A\}$*

Proof. If $(x, y), (x, y') \in f$ then there exists $a, a' \in A$ such that $(x, y) = (a, F(a)) \wedge (x, y') \in (a', F(a'))$, hence $x = a \wedge x = a' \wedge y = f(a) \wedge y' = F(a') \Rightarrow a = a' \wedge y' = F(a) \wedge y = F(a)$ proving that $y = y'$. So

$$f: A \rightarrow B \text{ is a partial function}$$

If $x \in A$ then as $F(x)$ is defined on every $x \in A$ we have that $(x, F(x)) \in f$ so that $x \in \operatorname{dom}(f)$. So $A \subseteq \operatorname{dom}(f)$ we have by 2.22 that

$$f: A \rightarrow B \;\text{ is a function} \qquad \square$$

This leads to a notation that we will gradually start to use

Notation 2.87. *The function definition $f: A \rightarrow B$ defined by $f(x) = F(x)$ [where $E(x)$ is a parameterized expression that calculates a unique value for every $x \in A$] is equivalent with*

$$f = \{z | z = (x, E x) \wedge x \in E\} = \{(x, E(x)) | x \in X\}$$

Example 2.88. $f: \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f(x) = \cos(4 \cdot x)$

2.3 Families

2.3.1 Family

We introduce now the idea of a indexed family which is essential a function of a class to another class. It is essential another notation for a function where the emphasis is on the objects in a collection and a way of indexing these objects and less on the function itself

Definition 2.89. *A Let I, B be classes then a family*

$$\boldsymbol{\{x_i\}_{i \in I} \subseteq B}$$

is actually a function

$$\boldsymbol{f: I \rightarrow B}$$

Further $\boldsymbol{x_i}$ is another notation for $\boldsymbol{f(i)}$ so that $\boldsymbol{y = f_i}$ is equivalent with $\boldsymbol{y = f(i)}$ or $\boldsymbol{(i, y) \in f}$

Note 2.90. In the above definition $\{x_i\}_{i \in I}$ only make sense if you specify what the defining function is. To avoid excessive notation, we assume that if we write $\boldsymbol{\{x\}_{i \in I} \subseteq B}$ that the defining function is $\boldsymbol{x: I \rightarrow B}$. However this is sometimes not feasible and in that case we state what the defining function of $\{x_i\}_{i \in I}$ is. Another way of specifying the associated function of a family is using [definition: 2.34] for a function as expressed in the following definition.

Definition 2.91. *Let I, B be classes then the family*

$$\boldsymbol{\{x_i\}_{i \in I} \subseteq B} \textit{\textbf{ defined by }} \boldsymbol{x_i = E(i)}$$

is the family defined by the function

$$\boldsymbol{f\colon I\rightarrow B \text{ defined by } f(i)=E(i)}$$

We can now define the concept of a sub family

Definition 2.92. *Let $\{A_i\}_{i\in I}\subseteq B$ be a family of objects in B defined by the function $f\colon I\rightarrow B$ and $J\subseteq I$ then $\{A_i\}_{i\in J}\subseteq B$ is the family defined by the function $f_{|J}\colon J\rightarrow B$ [see: theorem: 2.82 for the proof that $f_J\colon I\rightarrow B$ is a function]*

Definition 2.93. *Let I,J,A,B be classes such that $I\bigcap J=\varnothing$ and*

$$\{x\}_{i\in I}\subseteq A \text{ defined by the function } f\colon I\rightarrow A$$

$$\{y_i\}_{i\in J}\subseteq B \text{ defined by the function } g\colon J\rightarrow B$$

then $\{z_i\}_{i\in I\bigcup J}\subseteq A\bigcup B$ defined by $z_i=\left\{\begin{smallmatrix} A_i\text{if } i\in I\\ B_i \text{ if } i\in J\end{smallmatrix}\right.$ is the family defined by the function

$$f\bigcup g\colon I\bigcup J\rightarrow A\bigcup B$$

[see theorem: 2.74 for the proof that $f\bigcup g\colon I\bigcup J\rightarrow A\bigcup B$ is indeed a function]

Composition of functions can also also be represented via the above family notation,

Definition 2.94. *If you have a function $\boldsymbol{f\colon I\longrightarrow J}$ and a family $\boldsymbol{\{x_j\}_{j\in J}\subseteq A}$ [defined by the function $\boldsymbol{g\colon J\longrightarrow A}$] then*

$$\boldsymbol{\{x_{f(i)}\}_{i\in I}}$$

is the family represented by the function

$$\boldsymbol{g\circ f\colon I\longrightarrow A}$$

So a family is just another notation for a function. We introduce also a new notation for the range of this function.

Definition 2.95. *If $\{x_i\}_{i\in I}$ is a family of objects in B [standing for the function $f\colon I\rightarrow B$] then we define $\{x_i|i\in I\}$ by*

$$\{x_i|i\in I\}=\text{range}(f)$$

The motivation for this definition is the following theorem

Theorem 2.96. *If $\{x_i\}_{i\in I}\subseteq B$ is a family of objects in B with associated function f then*

$$x\in\{x_i|i\in I\}\Leftrightarrow\exists i\in I \text{ such that } x=x_i$$

Proof. As $\{x_i\}_{i\in I}\subseteq B$ is equivalent with $f\colon I\rightarrow B$ we have

$$\begin{array}{rcl} z\in\{x_i|i\in I\} & \underset{\text{define}}{\Leftrightarrow} & z\in\text{range}(x)\\ & \Leftrightarrow & \exists i \text{ with } (i,z)\in f\\ & \underset{f\subseteq I\times B}{\Leftrightarrow} & \exists i \text{ with } i\in I\wedge(i,z)\in f\\ & \Leftrightarrow & \exists i\in I \text{ with } (i,z)\in f\\ & \Leftrightarrow & \exists i\in I \text{ with } z=f(i)\\ & \Leftrightarrow & \exists i\in I \text{ with z=x\_i}\\ & & \Box \end{array}$$

Theorem 2.97. *If $\{x_i\}_{i\in I}\subseteq B$ is a family such that I and B are sets then $\{x_i|i\in I\}$ is a set*

Proof. $\{x_i\}_{i\in I}\subseteq B$ is actually the function $x\colon I\rightarrow B$ where $\text{range}(x)=\{x_i|i\in I\}$. As $I$and B are sets, it follows from [theorem: 2.11] that $\text{range}(x)$ is a set, hence $\{x_i|i\in I\}$ is a set. $\Box$

Up to now we consider a family as a indexed collection of objects. What is actually a object, in set theory it is a class which can be either a set or a proper class. A class is a collection so we can talk about the union of these collection. The convention is then to use upper case instead of lower case. If we want to deal with the union and intersection of the objects [considered as collections] in the family we use also a different notation.

Notation 2.98. *If $\{A_i\}_{i\in I}\subseteq B$ is a family of objects in B [standing for the function $A: I\rightarrow B$] then $\bigcup_{i\in I} A_i$ is defined by*

$$\bigcup_{i\in I} A_i = \bigcup \{\text{range}(A)\} \text{ [definition: 1.56]}$$

Definition 2.99. *A family $\{A_i\}_{i\in I}\subseteq B$ is **pairwise disjoint** iff $\forall i,j\in I$ with $i\neq j$ we have $A_i \bigcap A_j = \varnothing$.*

Notation 2.100. *If $\{A_i\}_{i\in I}\subseteq B$ is pairwise disjoint and we want to indicate this fact when we write the union of the family then we use the notation $\bigsqcup_{i\in I} A_i$. So $\bigsqcup_{i\in I} A_i$ is actually the same as $\bigcup_{i\in I} A_i$, but also relating the information that $\{A_i\}_{i\in I}$ is pairwise disjoint.*

Using this new notation we have the following characterization of the union

Theorem 2.101. *If $\{A_i\}_{i\in I}\subseteq B$ is a family of objects in B then*

$$x\in\bigcup_{i\in I} A_i \Leftrightarrow \exists i\in I \text{ such that } x\in A_i$$

Proof. As $\{A_i\}_{i\in I}\subseteq B$ is actually the function $A: I\rightarrow B$ where $\bigcup_{i\in I} A_i = \bigcup \text{range}(A)$. Then we have

$$\begin{array}{rcl}
x\in\bigcup_{i\in I} A_i & \underset{\text{definition}}{\Leftrightarrow} & x\in\bigcup \text{range}(A) \\
& \underset{\text{[definition: 1.56]}}{\Leftrightarrow} & \exists y\in\text{range}(A) \text{ such that } x\in y \\
& \Leftrightarrow & \exists i \text{ such that } (i,y)\in A \text{ and } x\in y \\
& \underset{A\subseteq I\times B}{\Leftrightarrow} & \exists i\in I \text{ such that } (x,y)\in A \text{ and } x\in y \\
& \Leftrightarrow & \exists i\in I \text{ such that } y=A_i \text{ and } x\in y \\
& \Leftrightarrow & \exists i\in I \text{ such that } x\in A_i
\end{array}$$

□

Corollary 2.102. *If $\{A_j\}_{j\in J}\subseteq B$ is a family and $f: I\rightarrow J$ is a surjection then*

$$\bigcup_{j\in J} A_j = \bigcup_{i\in I} A_{f(i)}$$

Proof. If $x\in\bigcup_{i\in J} A_j$ then by [theorem: 2.101] there exist a $j\in J$ such that $x\in A_j = A(j)$. As f is surjective we have by [theorem: 2.48] that there exist a $i\in I$ such that $j=f(i)$. Hence $x\in A(f(i)) = (A\circ f)(i)$. So by [theorem: 2.101] and the definition of $\bigcup_{i\in I} A_{f(i)}$ we have $x\in\bigcup_{i\in I} A_{f(i)}$. Hence

$$\bigcup_{j\in J} A_j \subseteq \bigcup_{i\in I} A_{f(i)} \tag{2.32}$$

If $x\in\bigcup_{i\in I} A_{f(i)}$ then there exist a $i\in I$ such that $x\in(A\circ f)(i)$, which, as using [theorem: 2.19] $(A\circ f)(i)\in\text{range}(A)$, means that there exists a $j\in J$ such that $A_j = (A\circ f)(i)$. Hence $x\in A_j$ proving by [theorem: 2.101] that $x\in\bigcup_{j\in J} A_j$. So $\bigcup_{i\in I} A_{f(i)}\subseteq\bigcup_{j\in J} A_j$ which combined with [eq: 2.32] gives

$$\bigcup_{j\in J} A_j = \bigcup_{i\in I} A_{f(i)}$$

□

Theorem 2.103. *If $\{A_i\}_{i\in I}\subseteq B$ is a family of objects in B where I and B are sets then $\bigcup_{i\in I} A_i$ is a set.*

Proof. As $\{A_i\}_{i\in I}\subseteq B$ is another way of saying $A: I\rightarrow B$ and I and B are sets, it follows from [theorem: 2.11] that $\mathrm{range}(A)$ is a set. Using the Axiom of Union [axiom: 1.61] $\bigcup \mathrm{range}(A)$ is a set, so by definition $\bigcup_{i\in I} A_i$. is a set. □

Example 2.104. Let $\{A_i\}_{i\in\varnothing}\subseteq B$ be the family defined by $A=\varnothing$ [the empty function $\varnothing: \varnothing\rightarrow B$ [see example: 2.39[] then $\bigcup_{i\in\varnothing} A_i=\varnothing$

Proof. Let $y\in\mathrm{range}(A)=\mathrm{range}(\varnothing)$ then x such that $(x,y)\in\varnothing$, a contradiction. Hence $\mathrm{range}(A)=\varnothing$. So

$$\bigcup_{i\in\varnothing} A=\bigcup \mathrm{range}(A)=\bigcup \varnothing \underset{1.58}{=} \varnothing$$ □

Definition 2.105. *If $\{A_i\}_{i\in I}\subseteq B$ is a family of objects in B [standing for the function $A: I\rightarrow B$] then $\bigcap_{i\in I} A_i$ is defined by*

$$\bigcap_{i\in I} A_i=\bigcap \mathrm{range}(A) \text{ [definition: 1.57]}$$

Theorem 2.106. *If $\{A_i\}_{i\in I}\subseteq B$ then $x\in\bigcap_{i\in I} A_i\Leftrightarrow\forall i\in I$ we have $x\in A_i$*

Proof. $\{A_i\}_{i\in I}\subseteq B$ is actually the function $A: I\rightarrow B$ where $\bigcap_{i\in I} A_i=\bigcap \mathrm{range}(A)$.

$$\begin{aligned}
x\in\bigcap_{i\in I} A_i &\underset{\text{definition}}{\Leftrightarrow} x\in\bigcap \mathrm{range}(A)\\
&\underset{\text{[definition: 1.57]}}{\Leftrightarrow} \forall y\in\mathrm{range}(A) \text{ we have } x\in y\\
&\underset{y\in\mathrm{range}(A)\Leftrightarrow\exists i \text{ with } (i,y)\in A}{\Leftrightarrow} \forall i\in I \text{ with } (i,y)\in A \text{ we have } x\in y\\
&\Leftrightarrow \forall i\in I \text{ with } y=A_i \text{ we have } x\in y\\
&\Leftrightarrow \forall i\in I \text{ we have } x\in A_i
\end{aligned}$$

□

Theorem 2.107. *If $\{A_i\}_{i\in I}\subseteq B$ is a family of objects in B such that $I\neq\varnothing$ then $\bigcap_{i\in I} A_i$ is a set.*

Proof. $\{A_i\}_{i\in I}\subseteq B$ is actually the function $A: I\rightarrow B$ where $\bigcap_{i\in I} A_i=\bigcap \mathrm{range}(A)$. As $I\neq\varnothing$ there exists a $i\in I$. Given that A is a function it follows that $\mathrm{dom}(A)=I$, so there exists a y such that $(i,y)\in A$ or $y\in\mathrm{range}(A)$. So $\varnothing\neq\mathrm{range}(A)$ which by [theorem: 1.57] proves that $\bigcap \mathrm{range}(A)$ is a set, hence $\bigcap_{i\in I} A_i$ is a set. □

Example 2.108. Let $I=\{0\}$, B a class and take $A: I\rightarrow\{B\}$ defined by $A=\{(0,B)\}$, defining the family $\{A_i\}_{i\in\{0\}}\subseteq\{B\}$ where $A_0=B$. For this family we have $\bigcap_{i\in\{0\}} A_i=B$ and $\bigcup_{i\in\{0\}} A_i=B$

Proof. Using [example: 2.61] it follows that $A: I\rightarrow\{B\}$ is bijection, hence a function, so that $\{A_i\}_{i\in\{0\}}\subseteq\{B\}$ is a well defined family. Further as A is a bijection we have that

$$\mathrm{range}(A)=\{B\}$$

Finally

$$\bigcup_{i\in\{0\}} A_i=\bigcup \mathrm{range}(A)=\bigcup \{B\} \underset{\text{[example: 1.58]}}{=} A$$

and

$$\bigcap_{i\in\{0\}} A_i=\bigcap \mathrm{range}(A)=\bigcap \{B\} \underset{\text{[example: 1.58]}}{=} A$$ □

Example 2.109. Let C,D classes, $I=\{0,1\}$ and take $A: I\rightarrow\{C,D\}$ defined by $A=\{(0,C),(1,D)\}$ [see example: 2.23], defining the family $\{A_i\}_{i\in\{0,1\}}\subseteq\{C,D\}$ where $A_0=C$ and $A_1=D$. For this family we have $\bigcup_{i\in\{0,1\}} A_i=C\bigcup D$ and $\bigcap_{i\in\{0,1\}} A_i=C\bigcap D$.

Proof. If $y \in \operatorname{range}(A)$ then $\exists x$ such that $(x, y) \in A = \{(0, C), (1, D)\}$, so that $(x, y) = (0, C) \Rightarrow y = C$ or $(x, y) = (1, D) \Rightarrow y = D$, proving that $x \in \{C, D\}$. Further if $y \in \{C, D\}$ then $y = C \Rightarrow (0, C) \in A \Rightarrow y \in \operatorname{range}(A)$ or $y = D \Rightarrow (1, D) \in A \Rightarrow y \in \operatorname{range}(A)$. So we have

$$\operatorname{range}(A) = \{C, D\}$$

Finally

$$\bigcup_{i \in \{0,1\}} A_i = \bigcup \operatorname{range}(A) = \bigcup \{C, D\} \underset{\text{[example: 1.59]}}{=} C \bigcup D$$

and

$$\bigcap_{i \in \{0,1\}} A_i = \bigcap \operatorname{range}(A) = \bigcap \{C, D\} \underset{\text{[example: 1.59]}}{=} C \bigcap D$$

□

2.3.2 Properties of the union and intersection of families

To save space, from now on we use [theorem: 2.101] and [theorem: 2.106] about union and intersection of families without explicit referring to these theorems.

Theorem 2.110. *If $\{A_i\}_{i \in I} \subseteq B$ is a family then we have:*

1. *$\forall i \in I$ we have $A_i \subseteq \bigcup_{i \in I} A_i$*
2. *$\forall i \in I$ we have $\bigcap_{i \in I} A_i \subseteq A_i$*
3. *If $\forall i \in I$ we have that $A_i \subseteq C$ then $\bigcup_{i \in I} A_i \subseteq C$*
4. *If $\forall i \in I$ we have $C \subseteq A_i$ then $C \subseteq \bigcap_{i \in I} A_i$*

Proof.

1. Let $i \in I$ and assume that $x \in A_i$ then $\exists i \in I$ such that $x \in A_i$, so $x \in \bigcup_{i \in I} A_i$, proving that $A_i \subseteq \bigcup_{i \in I} A_i$.
2. Let $i \in I$ then if $x \in \bigcap_{i \in I} A_i$ we have $\forall j \in I$ that $x \in A_j \underset{i \in I}{\Rightarrow} x \in A_i$, proving that $\bigcap_{i \in I} A_i \subseteq A_i$
3. $$\begin{aligned} x \in \bigcup_{i \in I} A_i &\Rightarrow \exists i \in I \vdash x \in A_i \\ &\underset{A_i \subseteq C}{\Rightarrow} x \in C \\ &\Rightarrow \bigcup_{i \in I} A_i \subseteq C \end{aligned}$$
4. $$\begin{aligned} x \in C &\Rightarrow \forall i \in I \vDash x \in A_i \\ &\Rightarrow x \in \bigcap_{i \in I} A_i \\ &\Rightarrow C \subseteq \bigcap_{i \in I} A_i \end{aligned}$$

□

Theorem 2.111. *If $\{A_i\}_{i \in I} \subseteq B$ is a family then*

1. *If $J \subseteq I$ then*
   a. *$\bigcup_{i \in J} A_i \subseteq \bigcup_{i \in I} A_i$*
   b. *$\bigcap_{i \in I} A_i \subseteq \bigcap_{i \in J} A_i$*
2. *If $I = J \bigcup K$ then*
   a. *$\bigcup_{i \in I} A_i = (\bigcup_{i \in J} A_i) \bigcup (\bigcup_{i \in K} A_i)$*
   b. *$\bigcap_{i \in I} A_i = (\bigcap_{i \in J} A_i) \bigcap (\bigcap_{i \in K} A_i)$*

Proof.

1.

   a. If $x \in \bigcup_{i \in J} A_i$ then $\exists i \in J$ such that $x \in A_i$, as $J \subseteq I$ we have $i \in I$ with $x \in A_i$, so that $x \in \bigcup_{i \in I} A_i$.

   b. If $x \in \bigcap_{i \in I} A_i$ then $\forall i \in I$ we have $x \in A_i$, as $J \subseteq I$ we have also $\forall i \in J$ that $x \in A_i$, hence $x \in \bigcap_{i \in J} A_i$.

2.

   a. As by [theorem: 1.25] $J, K \subseteq I$ we have using (1) that $\bigcup_{i \in J} A_i \subseteq \bigcup_{i \in I} A_i$ and $\bigcup_{i \in K} A_i \subseteq \bigcup_{i \in I} A_i$. Using [theorem: 1.25 it follows that

$$\left(\bigcup_{i \in J} A_i\right) \bigcup \left(\bigcup_{i \in K} A_i\right) \subseteq \bigcup_{i \in I} A_i \tag{2.33}$$

   If $x \in \bigcup_{i \in I} A$ then $\exists i \in I$ such that $x \in A_i$, as $I = J \bigcup K$ we have $i \in J \Rightarrow x \in \bigcup_{i \in J} A_i$ or $i \in K \Rightarrow x \in \bigcup_{i \in K} A_i$, which proves that $x \in (\bigcup_{i \in J} A_i) \bigcup (\bigcup_{i \in K} A_i)$. Hence

$$\bigcup_{i \in I} A_i \subseteq \left(\bigcup_{i \in J} A_i\right) \bigcup \left(\bigcup_{i \in K} A_i\right)$$

   which combined with [eq: 2.33] proves

$$\bigcup_{i \in I} A_i = \left(\bigcup_{i \in J} A_i\right) \bigcup \left(\bigcup_{i \in K} A_i\right)$$

   b. As by [theorem: 1.25] $J, K \subseteq I$ we have using (1) that $\bigcap_{i \in I} A_i \subseteq \bigcap_{i \in J} A_i$ and $\bigcap_{i \in I} A_i \subseteq \bigcap_{i \in K} A_i$. Using [theorem: 1.25] it follows that

$$\bigcap_{i \in I} A_i \subseteq \left(\bigcap_{i \in J} A_i\right) \bigcap \left(\bigcap_{i \in K} A_i\right) \tag{2.34}$$

   If $x \in (\bigcap_{i \in J} A) \bigcap (\bigcap_{i \in K} A)$ then $x \in \bigcap_{i \in J} A_i$ and $x \in \bigcap_{i \in K} A_i$. So $\forall i \in J$ we have $x \in A_i$ and $\forall i \in K$ we have $x \in A_i$. Hence as $\forall i \in I$ we have $i \in J \Rightarrow x \in A_i$ or $i \in K \Rightarrow x \in A_i$ it follows that $x \in \bigcap_{i \in I} A_i$. So $(\bigcap_{i \in J} A) \bigcap (\bigcap_{i \in K} A) \subseteq \bigcap_{i \in I} A_i$ which combined with [eq: 2.34] proves

$$\bigcap_{i \in I} A_i = \left(\bigcap_{i \in J} A_i\right) \bigcap \left(\bigcap_{i \in K} A_i\right)$$

□

Theorem 2.112. *Let* $\{A_i\}_{i \in I} \subseteq C$ *and* $\{B_i\}_{i \in I} \subseteq D$ *be two families such that* $\forall i \in I$ *we have* $A_i \subseteq B_i$ *then*

1. $\bigcup_{i \in I} A_i \subseteq \bigcup_{i \in I} B_i$
2. $\bigcap_{i \in I} A_i \subseteq \bigcap_{i \in I} B_i$

Proof.

1. If $x \in \bigcup_{i \in I} A_i$ there exist a $i \in I$ such that $x \in A_i \underset{A_i \subseteq B_i}{\Rightarrow} x \in B_i$, hence $x \in \bigcup_{i \in I} B_i$
2. If $x \in \bigcap_{i \in I} A_i$ then $\forall i \in I$ we have $x \in A_i \underset{A_i \subseteq B_i}{\Rightarrow} x \in B_i$ proving $x \in \bigcap_{i \in I} B_i$ □

We have also the distributive laws for union and intersection [theorem: 1.30]

Theorem 2.113. (Distributivity) *Let* $\{A_i\}_{i \in I} \subseteq B$ *be a family and* C *a class then*

1. $C \bigcap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (C \bigcap A_i)$

2. $C\bigcup\left(\bigcap_{i\in I}A_i\right)=\bigcap_{i\in I}\left(C\bigcup A_i\right)$

3. $C\bigcap\left(\bigcap_{i\in I}A_i\right)=\bigcap_{i\in I}\left(C\bigcap A_i\right)$

4. $C\bigcup\left(\bigcup_{i\in I}A_i\right)=\bigcup_{i\in I}\left(C\bigcup A_i\right)$

Proof.

1. If $x\in C\bigcap\left(\bigcup_{i\in I}A_i\right)$ then $x\in C$ and $x\in\bigcup_{i\in I}A_i\Rightarrow\exists i\in I$ such that $x\in A_i$. Hence $x\in C\bigcap A_i$, proving by [theorem: 2.110] that $x\in\bigcup_{i\in I}A_i$. So
$$C\bigcap\left(\bigcup_{i\in I}A_i\right)\subseteq\bigcup_{i\in I}\left(C\bigcap A_i\right)\tag{2.35}$$
If $x\in\bigcup_{i\in}\left(C\bigcap A_i\right)$ then there exist a $i\in I$ such that $x\in C$ and $x\in A_i\Rightarrow x\in\bigcup_{i\in I}A_i$, so $x\in C\bigcap\left(\bigcup_{i\in I}A_i\right)$, proving that $\bigcup_{i\in I}\left(C\bigcap A_i\right)\subseteq C\bigcap\left(\bigcup_{i\in I}A_i\right)$. Combining this with [eq: 2.35] proves
$$C\bigcap\left(\bigcup_{i\in I}A_i\right)=\bigcup_{i\in I}\left(C\bigcap A_i\right)$$

2. If $x\in C\bigcup\left(\bigcap_{i\in I}A_i\right)$ then we have the following cases to consider:

   $x\in C$. then $\forall i\in I$ we have $x\in C\bigcup A_i$ hence $x\in\bigcap_{i\in I}\left(C\bigcup A_i\right)$

   $x\in\bigcap_{i\in I}A_i$. then $\forall i\in I$ we have $x\in A_i$ hence $x\in\bigcap_{i\in I}\left(C\bigcup A_i\right)$

   which proves that
$$C\bigcup\left(\bigcap_{i\in I}A_i\right)\subseteq\bigcap_{i\in I}\left(C\bigcup A_i\right)\tag{2.36}$$
If $x\in\bigcap_{i\in I}\left(C\bigcup A_i\right)$ then we have two cases to consider:

   $x\in C$. then $x\in C\bigcup\left(\bigcap_{i\in I}A_i\right)$

   $x\notin C$. then, as $\forall i\in I$ we have $x\in C\bigcup A_i\underset{x\notin C}{\Rightarrow}x\in A_i$, it follows that $x\in\bigcap_{i\in I}A_i$ hence $x\in C\bigcup\left(\bigcap_{i\in I}A_i\right)$

   In all cases we have $x\in C\bigcup\left(\bigcap_{i\in I}A_i\right)$ proving that $\bigcap_{i\in I}\left(C\bigcup A_i\right)\subseteq C\bigcup\left(\bigcap_{i\in I}A_i\right)$, combining this with [eq: 2.36] gives
$$C\bigcup\left(\bigcap_{i\in I}A_i\right)\subseteq\bigcap_{i\in I}\left(C\bigcup A_i\right)$$

3. We have
$$\begin{aligned}x\in C\bigcap\left(\bigcap_{i\in I}A_i\right)&\Leftrightarrow x\in C\wedge\forall i\in I\text{ we have }x\in A_i\\&\Leftrightarrow\forall i\in I\text{ we have }x\in C\bigcap A_i\\&\Leftrightarrow x\in\bigcap_{i\in I}\left(C\bigcap A_i\right)\end{aligned}$$
Proving
$$C\bigcap\left(\bigcap_{i\in I}A_i\right)=\bigcap_{i\in I}\left(C\bigcap A_i\right)$$

4. We have
$$\begin{aligned}x\in C\bigcup\left(\bigcup_{i\in I}A_i\right)&\Leftrightarrow x\in C\vee x\in\bigcup_{i\in I}A_i\\&\Leftrightarrow x\in C\vee\exists i\in I\text{ with }x\in A_i\\&\Leftrightarrow\exists i\in I\text{ with }(x\in C\vee x\in A_i)\\&\Leftrightarrow\exists i\in I\text{ we have }x\in C\bigcup A_i\end{aligned}$$

proving that

$$C\bigcup\left(\bigcup_{i\in I}A_i\right)=\bigcup_{i\in I}(C\bigcup A_i)$$

□

Theorem 2.114. *Let $\{A_i\}_{i\in I}\subseteq C$ and $\{B_i\}_{i\in I}\subseteq D$ be two families then*

1. $(\bigcup_{i\in I}A_i)\bigcup(\bigcup_{i\in I}B_i)=\bigcup_{i\in I}(A_i\bigcup B_i)$
2. $\bigcup_{i\in I}(A_i\bigcap B_i)\subseteq(\bigcup_{i\in I}A_i)\bigcap(\bigcup_{i\in I}B_i)$

Proof.

1. First as $\forall i\in I$ we have by [theorem: 1.25] that $A_i\subseteq A_i\bigcup B_i$ and $B_i\subseteq A_i\bigcup B_i$ so it follows using [theorem: 2.112] that $\bigcup_{i\in I}A_i\subseteq\bigcup_{i\in I}(A_i\bigcup B_i)$ and $\bigcup_{i\in I}B_i\subseteq\bigcup_{i\in I}(A_i\bigcup B_i)$. Applying then [theorem: 1.25] gives

$$\left(\bigcup_{i\in I}A_i\right)\bigcup\left(\bigcup_{i\in I}B_i\right)\subseteq\bigcup_{i\in I}(A_i\bigcup B_i) \tag{2.37}$$

If now $x\in\bigcup_{i\in I}A_i\bigcup B_i$ then $\exists i\in I$ such that $x\in A_i\bigcup B_i$, then we have $x\in A_i\Rightarrow x\in\bigcup_{i\in I}A_i$ or $x\in B_i\Rightarrow x\in\bigcup_{i\in I}B_i$. So $x\in(\bigcup_{i\in I}A_i)\bigcup(\bigcup_{i\in I}B_i)$ proving that $\bigcup_{i\in I}(A_i\bigcup B_i)\subseteq(\bigcup_{i\in I}A_i)\bigcup(\bigcup_{i\in I}B_i)$ which combined with 2.37 gives

$$\left(\bigcup_{i\in I}A_i\right)\bigcup\left(\bigcup_{i\in I}B_i\right)=\bigcup_{i\in I}(A_i\bigcup B_i)$$

2. As $\forall i\in I$ we have by [theorem: 1.25] that $A_i\bigcap B_i\subseteq A_i$ and $A_i\bigcap B_i\subseteq A_i$, $B_i\subseteq A_i\bigcup B_i$ it follows using [theorem: 2.112] that $\bigcup_{i\in I}(A_i\bigcap B_i)\subseteq\bigcup_{i\in I}A_i$ and $\bigcup_{i\in I}(A_i\bigcap B_i)\subseteq\bigcup_{i\in I}B_i$. Using then [theorem: 1.25] we have

$$\bigcup_{i\in I}(A_i\bigcap B_i)\subseteq\left(\bigcup_{i\in I}A_i\right)\bigcup\left(\bigcup_{i\in I}B_i\right)$$

□

We have also a variant of the deMorgan's laws [theorem: 1.29]

Theorem 2.115. (deMorgan's Law) *Let $\{A_i\}_{i\in I}\subseteq B$ be a family then we have*

1. $(\bigcup_{i\in I}A_i)^c=\bigcap_{i\in I}(A_i)^c$
2. $(\bigcap_{i\in I}A_i)^c=\bigcup_{i\in I}(A_i)^c$
3. *If C is a class then $C\setminus(\bigcup_{i\in I}A_i)=\bigcap_{i\in I}(A_i\setminus C)$*
4. *If C is a class then $C\setminus(\bigcap_{i\in I}A_i)=\bigcup_{i\in I}(C\setminus A_i)$*

Proof.

1.

$$\begin{aligned}
x\in\left(\bigcup_{i\in I}A_i\right)^c &\Leftrightarrow x\notin\left(\bigcup_{i\in I}A_i\right)\\
&\Leftrightarrow \neg\left(x\in\bigcup_{i\in I}A_i\right)\\
&\Leftrightarrow \neg(\exists i\in I \text{ with } x\in A_i)\\
&\Leftrightarrow \forall i\in I \text{ we have } \neg(x\in A_i)\\
&\Leftrightarrow \forall i\in I \text{ we have } x\notin A_i\\
&\Leftrightarrow \forall i\in I \text{ we have } x\in(A_i)^c\\
&\Leftrightarrow x\in\bigcap_{i\in I}(A_i)^c
\end{aligned}$$

proving that

$$\left(\bigcup_{i\in I} A_i\right)^c = \bigcap_{i\in I} (A_i)^c$$

2.

$$\begin{aligned} x\in\left(\bigcap_{i\in I} A_i\right)^c &\Leftrightarrow x\notin\left(\bigcap_{i\in I} A_i\right)^c \\ &\Leftrightarrow \neg\left(x\in\left(\bigcap_{i\in I} A_i\right)\right) \\ &\Leftrightarrow \neg(\forall i\in I \text{ we have } x\in A_i) \\ &\Leftrightarrow \exists i\in I \text{ we have } \neg(x\in A_i) \\ &\Leftrightarrow \exists i\in I \text{ we have } x\notin A_i \\ &\Leftrightarrow \exists i\in I \text{ we have } x\in (A_i)^c \\ &\Leftrightarrow x\in\bigcup_{i\in I} (A_i)^c \end{aligned}$$

proving that

$$\left(\bigcap_{i\in I} A_i\right)^c = \bigcup_{i\in I} (A_i)^c$$

3. We have

$$\begin{aligned} C\setminus\left(\bigcup_{i\in I} A_i\right) &\underset{[\text{theorem: } 1.24]}{=} C\bigcap\left(\bigcup_{i\in I} A_i\right)^c \\ &\underset{(1)}{=} C\bigcap\left(\bigcap_{i\in I} (A_i)^c\right) \\ &\underset{[\text{theorem: } 2.113]}{=} \bigcap_{i\in I}\left(C\bigcap (A_i)^c\right) \\ &\underset{[\text{theorem: } 1.24]}{=} \bigcap_{i\in I} (C\setminus A_i) \end{aligned}$$

4. We have

$$\begin{aligned} C\setminus\left(\bigcap_{i\in I} A_i\right) &\underset{[\text{theorem: } 1.24]}{=} C\bigcap\left(\bigcap_{i\in I} A_i\right)^c \\ &\underset{(2)}{=} C\bigcap\left(\bigcup_{i\in I} (A_i)^c\right) \\ &\underset{[\text{theorem: } 2.113]}{=} \bigcup_{i\in I}\left(C\bigcap (A_i)^c\right) \\ &= \bigcup_{i\in I} (C\setminus A_i) \end{aligned}$$

□

Theorem 2.116. *If $\{A_i\}_{i\in I}\subseteq B$ is a family and A a class then we have*

1. $(\bigcup_{i\in I} A_i)\setminus A = \bigcup_{i\in I} (A_i\setminus A)$
2. $(\bigcap_{i\in I} A_i)\setminus A = \bigcap_{i\in I} (A_i\setminus A)$
3. $(\bigcup_{i\in I} A_i)\times A = \bigcup_{i\in I} (A_i\times A)$
4. $A\times(\bigcup_{i\in I} A_i) = \bigcup_{i\in I} (A\times A_i)$
5. $(\bigcap_{i\in I} A_i)\times A = \bigcap_{i\in I} (A_i\times A)$
6. $A\times(\bigcap_{i\in I} A_i) = \bigcap_{i\in I} (A\times A_i)$

Proof.

1.

$$\begin{aligned}
\left(\bigcup_{i\in I} A_i\right)\setminus A &\underset{[\text{theorem: } 1.24]}{=} \left(\bigcup_{i\in I} A_i\right)\bigcap A^c \\
&\underset{[\text{theorem: } 1.30]}{=} A^c\bigcap\left(\bigcup_{i\in I} A_i\right) \\
&\underset{[\text{theorem: } 2.113]}{=} \bigcup_{i\in I}\left(A^c\bigcap A_i\right) \\
&\underset{[\text{theorem: } 1.30]}{=} \bigcup_{i\in I}\left(A_i\bigcap A^c\right) \\
&\underset{[\text{theorem: } 1.24]}{=} \bigcup_{i\in I}\left(A_i\setminus A\right)
\end{aligned}$$

2.

$$\begin{aligned}
\left(\bigcap_{i\in I} A_i\right)\setminus A &\underset{[\text{theorem: } 1.24]}{=} \left(\bigcap_{i\in I} A_i\right)\bigcap A^c \\
&\underset{[\text{theorem: } 1.30]}{=} A^c\bigcap\left(\bigcap_{i\in I} A_i\right) \\
&\underset{[\text{theorem: } 2.113]}{=} \bigcap_{i\in I}\left(A^c\bigcap A_i\right) \\
&\underset{[\text{theorem: } 1.30]}{=} \bigcap_{i\in I}\left(A_i\bigcap A^c\right) \\
&\underset{[\text{theorem: } 1.24]}{=} \bigcap_{i\in I}\left(A_i\setminus A\right)
\end{aligned}$$

3.

$$\begin{aligned}
(x,y)\in\left(\bigcup_{i\in I} A_i\right)\times A &\Leftrightarrow x\in\bigcup_{i\in I} A_i\wedge y\in A \\
&\Leftrightarrow y\in A\wedge\exists i\in I \text{ with } x\in A_i \\
&\Leftrightarrow \exists i\in I \text{ with } (x\in A_i\wedge y\in A) \\
&\Leftrightarrow \exists i\in I \text{ with } (x,y)\in A_i\times A \\
&\Leftrightarrow (x,y)\in\bigcup_{i\in I}(A_i\times A)
\end{aligned}$$

4.

$$\begin{aligned}
(x,y)\in A\times\left(\bigcup_{i\in I} A_i\right) &\Leftrightarrow x\in A\wedge y\in\bigcup_{i\in I} A_i \\
&\Leftrightarrow x\in A\wedge\exists i\in I \text{ with } y\in A_i \\
&\Leftrightarrow \exists i\in I \text{ with } (x\in A\wedge y\in A_i) \\
&\Leftrightarrow \exists i\in I \text{ with } (x,y)\in A\times A_i \\
&\Leftrightarrow (x,y)\in\bigcup_{i\in I}(A\times A_i)
\end{aligned}$$

5.

$$\begin{aligned}
(x,y)\in\left(\bigcap_{i\in I} A_i\right)\times A &\Leftrightarrow x\in\bigcap_{i\in I} A_i\wedge y\in A \\
&\Leftrightarrow (\forall i\in I \text{ we have } x\in A_i)\wedge y\in A \\
&\Leftrightarrow \forall i\in I \text{ we have } (x\in A_i\wedge y\in A) \\
&\Leftrightarrow \forall i\in I \text{ we have } (x,y)\in A_i\times A \\
&\Leftrightarrow (x,y)\in\bigcap_{i\in I}(A_i\times A)
\end{aligned}$$

6.

$$\begin{aligned}(x,y)\in A\times\left(\bigcap_{i\in I}A_i\right) &\Leftrightarrow x\in A\wedge y\in\bigcap_{i\in I}A_i\\ &\Leftrightarrow (\forall i\in I \text{ we have } y\in A_i)\wedge x\in A\\ &\Leftrightarrow \forall i\in I \text{ we have } (y\in A_i\wedge x\in A)\\ &\Leftrightarrow \forall i\in I \text{ we have } (x,y)\in A\times A_i\\ &\Leftrightarrow (x,y)\in\bigcap_{i\in I}(A\times A_i)\end{aligned}$$

□

Theorem 2.117. *Let $\{A_i\}_{i\in I}\subseteq B$ a family then*

1. *If $j\in I$ then $\left(\bigcup_{i\in I\setminus\{j\}}A_i\right)\bigcup A_j=\bigcup_{i\in I}A_i$*
2. *$\bigcup_{i\in I}A_i=\bigcup_{i\in\{j\in I|A_j\neq\varnothing\}}A_i$*
3. *If $\exists i\in I$ such that $A_i=\varnothing$ then $\bigcap_{i\in I}A_i=\varnothing$*

Proof.

1. If $x\in\left(\bigcup_{i\in I\setminus\{j\}}A_i\right)\bigcup A_j$ then either $x\in A_j\subseteq\bigcup_{i\in I}A_i$ [see: 2.110], so that $x\in\bigcup_{i\in I}A_i$ or $x\in\bigcup_{i\in I\setminus\{j\}}A_i\Rightarrow\exists k\in I\setminus\{j\}$ with $x\in A_k$ which as $k\in I$ proves $x\in\bigcup_{i\in I}A_i$. If $x\in\bigcup_{i\in I}A_i$ then $\exists i\in I$ such that $x\in A_i$, we have then for i either $i\in I\setminus\{j\}$ so that $x\in\bigcup_{i\in I\setminus\{j\}}A_i$ or $i=j$ giving $x\in A_j$, proving that $x\in\left(\bigcup_{i\in I\setminus\{j\}}A_i\right)\bigcup A_j$.

2. As $\{j\in I|A_j\neq\varnothing\}\subseteq I$ we have by [theorem: 2.111] that

$$\bigcup_{i\in\{j\in I|A_j\neq\varnothing\}}A_i\subseteq\bigcup_{i\in I}A_i \tag{2.38}$$

   Further if $x\in\bigcup_{i\in I}A_i$ then there exist a $i\in I$ such that $x\in A_i$. As $x\in A_i$ we must have that $A_i\neq\varnothing$ or $i\in\{j\in I|A_j\neq\varnothing\}$, proving that $x\in\bigcup_{i\in\{j\in I|A_j\neq\varnothing\}}A_i$. So

$$\bigcup_{i\in I}A_i\subseteq\bigcup_{i\in\{j\in I|A_j\neq\varnothing\}}A_i$$

   combining this with [eq: 2.38] proves

$$\bigcup_{i\in I}A_i\subseteq\bigcup_{i\in\{j\in I|A_j\neq\varnothing\}}A_i$$

3. Assume that $i\in I$ such that $A_i=\varnothing$. If $x\in\bigcap_{j\in I}A_j$ we have $\forall j\in I$ that $x\in A_j$, so for sure $x\in A_i$ which contradicts $A_i=\varnothing$. Hence we have that $\bigcap_{j\in I}A_j=\varnothing$.

□

Theorem 2.118. *If $f\colon A\to B$ is a function, $\{A_i\}_{i\in}\subseteq\mathcal{P}(A)$ and $\{B_i\}_{i\in I}\subseteq\mathcal{P}(B)$ are families of sub-classes of A and B then*

1. *$f(\bigcup_{i\in I}A_i)=\bigcup_{i\in I}f(A_i)$*
2. *$f^{-1}(\bigcup_{i\in I}B_i)=\bigcup_{i\in I}f^{-1}(B_i)$*
3. *$f(\bigcap A_{i\in I})\subseteq\bigcap_{i\in I}f(A_i)$*
4. *If f is injective and $I\neq\varnothing$ then $f(\bigcap_{i\in I}A_i)=\bigcap_{i\in I}f(A_i)$*
5. *$f^{-1}(\bigcap_{i\in I}B_i)=\bigcup_{i\in I}f^{-1}(B_i)$*

Proof.

1. If $y\in f(\bigcup_{i\in I} A_i)$ then $\exists x\in\bigcup_{i\in I} A_i$ such that $(x,y)\in f$, hence $\exists i\in I$ such that $x\in A_i$, which as $(x,y)\in f$ proves that $y\in f(A_i)$. So $y\in\bigcup_{i\in I} f(A_i)$ giving
$$f\left(\bigcup_{i\in I} A_i\right)\subseteq\bigcup_{i\in I} f(A_i) \tag{2.39}$$
If $y\in\bigcup_{i\in I} f(A_i)$ then there exists a $i\in I$ such that $y\in f(A_i)$, hence $\exists x\in A_i$ such that $(x,y)\in f$, as $x\in A_i$ this implies $x\in\bigcup_{i\in I} A_i$, so we have that $y\in f(\bigcup_{i\in I} A_i)$. Hence $\bigcup_{i\in I} f(A_i)\subseteq f(\bigcup_{i\in I} A_i)$, which combined with [eq: 2.39] gives
$$f\left(\bigcup_{i\in I} A_i\right)=\bigcup_{i\in I} f(A_i)$$

2. If $x\in f^{-1}(\bigcup_{i\in I} B_i)$ then there exists a $y\in\bigcup_{i\in I} B_i$ such that $(x,y)\in f$, hence $\exists i\in I$ such that $y\in B_i$. So $x\in f^{-1}(B_i)$ which as $i\in I$ implies that $x\in\bigcup_{i\in I} f^{-1}(B_i)$ or
$$f^{-1}\left(\bigcup_{i\in I} B_i\right)\subseteq\bigcup_{i\in I} f^{-1}(A_i) \tag{2.40}$$
If $x\in\bigcup_{i\in I} f^{-1}(A_i)$ then there exists a $i\in I$ such that $x\in f^{-1}(A_i)$, so $\exists y\in A_i$ with $(x,y)\in f$. As from $y\in A_i$ we have $y\in\bigcup_{i\in I}$ it follows that $x\in f^{-1}(\bigcup_{i\in I} A_i)$. This proves that $\bigcup_{i\in I} f^{-1}(A_i)\subseteq f^{-1}(\bigcup_{i\in I} A_i)$ which combined with [eq: 2.40] gives
$$f^{-1}\left(\bigcup_{i\in I} B_i\right)=\bigcup_{i\in I} f^{-1}(B_i)$$

3. If $y\in f(\bigcap_{i\in I} A_i)$ then there exists a $x\in\bigcap_{i\in I} A_i$ such that $(x,y)\in f$. From $x\in\bigcap_{i\in I} A_i$ it follows that $\forall i\in I\, x\in A_i$, which as $(x,y)\in f$ proves that $\forall i\in I\, x\in f(A_i)$ or $x\in\bigcap_{i\in I} f(A_i)$. So
$$f\left(\bigcap_{i\in I} A_i\right)\subseteq\bigcap_{i\in I} f(A_i)$$

4. Let $y\in\bigcap_{i\in I} f(A_i)$ then $\forall i\in I$ we have $y\in f(A_i)$. As $I\neq\varnothing$ there exists a $i\in I$ and we must thus have that $y\in f(A_i)$. So there exists a $x\in A_i$ such that $(x,y)\in f$. Assume that $x\notin\bigcap_{i\in I} A_i$ then $\exists j\in I$ such that $x\notin A_j$. However as $j\in I$ we must have that $y\in f(A_j)$, so there exists a $x'\in A_j$ such that $(x',y)\in f$. As f is injective and $(x,y),(x',y)\in f$ we must have $x=x'$, but this means that $x\in A_j$ contradicting $x\notin A_j$. So the assumption that $x\notin\bigcap_{i\in I} A_i$ is wrong, hence $x\in\bigcap A_i$. As $(x,y)\in f$ we have $y\in f(\bigcap_{i\in I} A_i)$, proving that $\bigcap_{i\in I} f(A_i)\subseteq f(\bigcap_{i\in I} A_i)$, which combined with (3) proves
$$f\left(\bigcap_{i\in I} A_i\right)=\bigcap_{i\in I} f(A_i)$$

5. If $x\in f^{-1}(\bigcap_{i\in I} B_i)$ then there exists a $y\in\bigcap_{i\in I} B_i$ such that $(x,y)\in f$. Hence $\forall i\in I$ we have that $y\in B_i \underset{(x,y)\in f}{\Rightarrow} x\in f^{-1}(B_i)$ proving that $x\in\bigcap_{i\in I} f^{-1}B_i$. So
$$f^{-1}\left(\bigcap_{i\in I} B_i\right)\subseteq\bigcap_{i\in I} f^{-1}(B_i) \tag{2.41}$$
If $x\in\bigcap_{i\in I} f^{-1}(B_i)$ then $\forall i\in I$ we have $x\in f^{-1}(B_i)$ or $\exists y\in B_i$ with $(x,y)\in f$. So $y\in\bigcap_{i\in I} B_i$ which as $(x,y)\in f$ proves that $x\in f^{-1}(\bigcap_{i\in I} B_i)$. So $\bigcap_{i\in I} f^{-1}(B_i)\subseteq f^{-1}(\bigcap_{i\in I} B_i)$ which combined with 2.41 gives
$$f^{-1}\left(\bigcap_{i\in I} B_i\right)=\bigcup_{i\in I} f^{-1}(B_i)$$
□

2.4 Product of a family of sets

The Cartesian product $A\times B$ consists of all the possible pairs that you can form, where the first element is a element of A and the second element is a element of B. We want now to construct a generalized product of a family of classes consisting of tuples whose elements are indexed by the index of the family.

Definition 2.119. (Product of a family of sets) *Let $\{A_i\}_{i\in I}\subseteq B$ a family then the* ***product of $\{A_i\}_{i\in I}$*** *noted as $\prod_{i\in I} A_i$ is defined by*

$$\prod_{i\in I} A_i = \left\{ f : f \in \left(\bigcup_{i\in I} A_i\right)^I \text{ where } \forall i\in I \text{ we have } f(i)\in A_i \right\}$$

If $x\in\prod_{i\in I} A_i$ then x_i is defined as

$$x_i = x(i)$$

Here $(\bigcup_{i\in I} A_i)^I$ is the class of function graphs of functions between I and $\bigcup_{i\in I} A_i$ [definition: 2.25] and $f(i)$ is the unique y such that $(i,y)\in f$. So $\prod_{i\in I} A_i$ is the class of graphs of functions from I to $\bigcup_{i\in I} A_i$ such that $\forall i\in I$ $f_i = f(i)\in A_i$.

The following shows that the product of a family of only one class is 'almost' that class itself.

Example 2.120. Let $\{A_i\}_{i\in\{0\}}\subseteq\{B\}$ be the family in [example: 2.108] defined by $A:\{0\}\to\{B\}$ where $A=\{(0,B)\}$ then there exists a bijection between B and $\prod_{i\in\{0\}} A_i$ or as $A_0 = B$ there exists a bijection between A_0 and $\prod_{i\in\{0\}} A_i$.

Proof. First using [example: 2.108] we have

$$B = \bigcup_{i\in\{0\}} A_i \tag{2.42}$$

hence

$$\left(\bigcup_{i\in\{0\}} A_i\right)^{\{0\}} = B^{\{0\}} \tag{2.43}$$

Let $f\in B^{\{0\}} \underset{[\text{eq: } 2.43]}{=} \left(\bigcup_{i\in\{0\}} A_i\right)$ then if $i\in\{0\}$ we must have $i=1$ hence $f(i)=f(0)\in B = A(0) = A_0$ proving that $\forall i\in\{0\}$ we have $f(i)\in A_i$. Hence $f\in\prod_{i\in\{0\}} A_i$ from which it follows that $B^{\{0\}}\subseteq\prod_{i\in\{0\}} A_i$. As clearly $\prod_{i\in\{0\}} A_i\subseteq\left(\bigcup_{i\in\{0\}} A_i\right)^{\{0\}} \underset{[\text{eq: } 2.43]}{=} B^{\{0\}}$ we have that

$$\prod_{i\in\{0\}} A_i = B^{\{0\}}$$

Now by [theorem: 2.70] there exists a bijection between B and $B^{\{0\}}$ which by the above proves the example. □

The next theorem shows that the product of a family of two classes is 'almost' the Cartesian product of these classes.

Theorem 2.121. *Let $\{A_i\}_{i\in\{0,1\}}\subseteq\{C,D\}$ be the family in [example: 2.109] defined by $A:\{0,1\}\to\{C,D\}$ where $A=\{(0,C),(1,D)\}$ then there exists a bijection between $A\times B$ and $\prod_{i\in\{0,1\}} A_i$*

Proof. First using [example: 2.109]: we have that

$$\bigcup_{i\in\{0,1\}} A_i = C\bigcup D \tag{2.44}$$

so that

$$\left(\bigcup_{i\in\{0,1\}} A_i\right)^{\{0,1\}} = \left(C\bigcup D\right)^{\{0,1\}} \tag{2.45}$$

So

$$\prod_{i\in\{0,1\}} A_i = \left\{ f \mid f\in\left(C\bigcup D\right)^{\{0,1\}} \text{ where } f(0)\in C\wedge f(1)\in D \right\} \tag{2.46}$$

Given $(c,d)\in C\times D\Rightarrow c\in C\wedge d\in D$, define $f_{c,d}=\{(0,c),(1,d)\}$. If $(x,y)\in f_{c,d}$ we have either

$$(x,y)=(0,c)\Rightarrow x=0\in\{0,1\}\wedge y=c\in C\subseteq C\bigcup D\Rightarrow(x,y)\in\{0,1\}\times\left(C\bigcup D\right)$$

or

$$(x,y)=(1,d)\Rightarrow x=1\in\{0,1\}\wedge y=d\in D\subseteq C\bigcup D\Rightarrow(x,y)\in\{0,1\}\times\left(C\bigcup D\right)$$

proving that

$$f_{a,b}\subseteq\{0,1\}\times\left(C\bigcup D\right)\wedge f_{a,b}(0)\in C\wedge f_{a,b}(1)\in D \tag{2.47}$$

If $(x,y),(x,y')\in f_{c,d}$ then either

$$(x,y)=(0,c)\Rightarrow x=0\Rightarrow(0,y')\in f_{c,d}\Rightarrow(0,y')=(0,c)\Rightarrow y'=c\Rightarrow y=y'$$

or

$$(x,y)=(1,d)\Rightarrow x=1\Rightarrow(1,y')\in f_{c,d}\Rightarrow(1,y')=(1,d)\Rightarrow y'=d\Rightarrow y=y'.$$

Together with [eq: 2.47] this proves that

$$f_{a,b}\colon\{0,1\}\rightarrow C\bigcup D\text{ is a partial function} \tag{2.48}$$

If $x\in\{0,1\}$ then either $x=0\Rightarrow(0,c)\in f_{c,d}$ or $x=1\Rightarrow(1,d)\in f_{c,d}$ proving that $\{0,1\}\subseteq\mathrm{dom}(f_{c,d})$ which by [theorem: 2.22] proves that

$$f_{c,d}\colon\{0,1\}\rightarrow C\bigcup D\text{ is a function} \tag{2.49}$$

As by [eq: 2.47] $f_{c,d}(0)\in C\wedge f_{c,d}(1)\in D$ proving that

$$f_{c,d}\in\prod_{i\in\{0,1\}}A_i \tag{2.50}$$

Define now γ by $\gamma=\{((c,d),f_{c,d})|(c,d)\in C\times D\}$. If $(x,y)\in\gamma$ then $x=(c,d)\in C\times D$ and $y=f_{c,d}\underset{[\text{eq: }2.50]}{\Rightarrow}$, hence $y\in(C\bigcup D)^{\{0,1\}}$. This proves that $(x,y)\in(C\times D)\times\left(\prod_{i\in\{0,1\}}A_i\right)$ or

$$\gamma\subseteq(C\times D)\times\left(\prod_{i\in\{0,1\}}A_i\right) \tag{2.51}$$

If $(x,y),(x,y')\in\gamma$ then $\exists(c,d)\in C\times D$ such that $(x,y)=((c,d),f_{c,d})$ and $(x,y')=((c,d),f_{c,d})$ so that $y=f_{c,d}=y'$ hence $y=y'$. Combining this with [eq:2.51] proves that

$$\gamma\colon C\times D\rightarrow\left(\prod_{i\in\{0,1\}}A_i\right)\text{ is a partial function} \tag{2.52}$$

If $(c,d)\in C\times D$ then by definition of γ we have $((c,d),f_{c,d})\in\gamma$ so that $(c,d)\in\mathrm{dom}(\gamma)$ proving that $C\times D\subseteq\mathrm{dom}(\gamma)$. By [theorem: 2.22] and [eq: 2.52] we have

$$\gamma\colon C\times D\rightarrow\left(\prod_{i\in\{0,1\}}A_i\right)\text{ is a function} \tag{2.53}$$

If $(x,y),(x',y)\in\gamma$ then there exists $(c,d),(c',d')\in C\times D$ such that $x=(c,d)\wedge x'=(c',d')$ and $f_{c,d}=y=f_{c',d'}$. As $(0,c)\in f_{c,d}=f_{c',d'}$ we have $(0,c)=(0,c')$ giving $c=c'$ and from $(1,d)\in f_{c,d}=f_{c',d'}$ we have $(1,d)=(1,d')$ giving $d=d'$. So $(c,d)=(c',d')$ proving that

$$\gamma\colon C\times D\rightarrow\left(\prod_{i\in\{0,1\}}A_i\right)\text{ is a injection}$$

If $g\in\prod_{i\in\{0,1\}}A_i$ then $g\colon\{0,1\}\rightarrow C\bigcup D$ is a function and $g(0)\in C\wedge g(1)\in D$ So there exists a $c\in C$ such that $(0,c)\in g$ and there exists a $d\in D$ such that $(1,d)\in g$. So $g=\{(0,c),(1,d)\}=f_{c,d}$ which proves that

$$\gamma\colon C\times D\rightarrow\left(\prod_{i\in\{0,1\}}A_i\right)\text{ is a surjection}$$

□

Theorem 2.122. *Let $\{A_i\}_{i\in I}\subseteq A$ and $\{B_i\}_{i\in I}\subseteq B$ classes such that $\forall i\in I$ $A_i\subseteq B_i$ then*

$$\prod_{i\in I} A_i\subseteq\prod_{i\in I} B_i$$

Proof. Let $x\in\prod_{i\in I}A_i$ then $x\in(\bigcup_{i\in I}A_i)^I$ and $\forall i\in I$ $x(i)\in A_i$. Using [theorem: 2.112] it follows that $\bigcup_{i\in I}A_i\subseteq\bigcup_{i\in I}B_i$, applying [theorem: 2.29] proves then $(\bigcup_{i\in I}A_i)^I\subseteq(\bigcup_{i\in I}B_i)^I$, so that

$$x\in\left(\bigcup_{i\in I} B_i\right)^I$$

If $i\in I$ then $x(i)\in A_i$, which as $A_i\subseteq B_i$ gives $x(i)\in B_i$, combining this with the above proves that $x\in\prod_{i\in I}B_i$. Hence we have

$$\prod_{i\in I} A_i\subseteq\prod_{i\in I} B_i$$ □

Theorem 2.123. *Let $\{A_i\}_{i\in I}\subseteq C$ and $\{B_i\}_{i\in I}\subseteq D$ are two families then*

$$\left(\prod_{i\in I} A_i\right)\bigcap\left(\prod_{i\in I} B_i\right)=\prod_{i\in I}\left(A_i\bigcap B_i\right)$$

Proof. First, as $\forall i\in I$ we have by [theorem: 1.25] $A_i\bigcap B_i\subseteq A_i$ and $A_i\bigcap B_i\subseteq B_i$ it follows that by [theorem: 2.122]

$$\prod_{i\in I}\left(A_i\bigcap B_i\right)\subseteq\prod_{i\in I} A_i \text{ and } \prod_{i\in I}\left(A_i\bigcap B_i\right)\subseteq\prod_{i\in I} B_i$$

so that by [theorem: 1.25]

$$\prod_{i\in I}\left(A_i\bigcap B_i\right)\subseteq\left(\prod_{i\in I} A_i\right)\bigcap\left(\bigcup_{i\in I} B_i\right) \tag{2.54}$$

Now for the opposite inclusion Let $x\in(\prod_{i\in I}A_i)\bigcap(\prod_{i\in I}B_i)$ then $x\in\prod_{i\in I}A_i$ and $x\in\prod_{i\in I}B_i$. So $x\in(\bigcup_{i\in I}A_i)^I\wedge\forall i\in I\vDash x(i)\in A_i$ and $x\in(\bigcup_{i\in I}B_i)^I\wedge\forall i\in I\vDash x(i)\in B_i$. Hence

$$\begin{aligned} x\colon I\rightarrow\bigcup_{i\in I} A_i &\quad \text{is a function}\\ x\colon I\rightarrow\bigcup_{i\in I} B_i &\quad \text{is } a \text{ function}\\ \forall i\in I &\quad \text{we have } x(i)\in A_i\bigcap B_i \end{aligned}$$

Now if $(i,y)\in x$ we have $i\in I$ [as $x\subseteq I\times(\bigcup_i A_i)$] and $y=x(i)\in A_i\bigcap B_i\subseteq\bigcup_{i\in I}(A_i\bigcap B_i)$ so that $(i,y)\in I\times(\bigcup_{i\in I}(A_i\bigcap B_i))$ giving

$$x\subseteq I\times\left(\bigcup_{i\in I}\left(A_i\bigcap B_i\right)\right) \text{ and } \forall i\in I \text{ we have } x(i)\in A_i\bigcap B_i \tag{2.55}$$

Further as $x\colon I\rightarrow\bigcup_{i\in I}A_i$ is a function we have $\forall(i,y),(i,y')$ that $y=y'$ and that $\mathrm{dom}(x)=I$. Combining this with [eq: 2.55] proves that $f\colon I\rightarrow\bigcup_{i\in I}(A_i\times B_i)$ is a function and $\forall i\in I$ we have $x(i)\in A_i\bigcap B_i$. This proves that $x\in\prod_{i\in I}(A_i\bigcap B_i)$ giving $(\prod_{i\in I}A_i)\bigcap(\prod_{i\in I}B_i)\subseteq\prod_{i\in I}(A_i\bigcap B_i)$ which combined with 2.54 gives finally

$$\prod_{i\in I}\left(A_i\bigcap B_i\right)\subseteq\left(\prod_{i\in I} A_i\right)\bigcap\left(\bigcup_{i\in I} B_i\right)$$ □

The following theorem is a motivation for the notation A^B for the graphs of functions from B to A.

Theorem 2.124. *Let I, B be classes and consider the family $\{A_i\}_{i\in I}\subseteq\{B\}$ based on the constant function $A: I\rightarrow\{B\}$ where $A = C_B = I\times\{B\}$ so that $\forall i\in I$ $A(i) = B$ [see example: 2.40] then $\prod_{i\in I} A_i = A^I$*

Proof. For I we have the following cases to consider:

***I* = ∅.** Using [example: 2.27] we have that

$$\left(\bigcup_{i\in\varnothing} A_i\right)^{\varnothing} = \{\varnothing\}$$

Further $\forall i\in\varnothing$ we have $\varnothing(i)\in A_i$ is satisfied vacuously proving that $\varnothing\in\prod_{i\in\varnothing} A_i$ so that $\{\varnothing\}\subseteq\prod_{i\in\varnothing} A_i\subseteq(\bigcup_{i\in\varnothing} A_i)^{\varnothing} = \{\varnothing\}$ or taking $I = \varnothing$

$$\prod_{i\in I} A_i = A^I$$

***I* ≠ ∅.** If $y\in\operatorname{range}(A)$ then $\exists x$ such that $(x, y)\in C_B = I\times\{B\}$, so that $y\in\{B\}$. Hence

$$\operatorname{range}(A)\subseteq\{B\} \tag{2.56}$$

As $I\neq\varnothing$ there exists a $i\in I$, which by the definition of C_B means that $(i, B)\in C_B$, hence $B\in\operatorname{range}(A)$. So if $y\in\{B\}$ then $y = B\in\operatorname{range}(A)$ proving that $\{B\}\subseteq\operatorname{range}(A)$ which combined with [eq: 2.56] gives

$$\operatorname{range}(A) = \{B\}$$

hence

$$\bigcup_{i\in I} A_i = \bigcup(\operatorname{range}(A)) = \bigcup\{B\} \underset{\text{[example: 1.58]}}{=} B$$

so that

$$\left(\bigcup_{i\in I} A_i\right)^I = B^I \tag{2.57}$$

Now if $f\in B^I$ then $\forall i\in I$ we have $f(i)\in B = A(i) = A_i$ proving that

$$f\in\{f|f\in B^i\wedge\forall i\in I f(i)\in A_i\} \underset{\text{[eq: 2.57]}}{=} \left\{f|f\in\left(\prod_{i\in I} A_i\right)^I\wedge\forall i\in I f(i)\in A_i\right\} = \prod_{i\in I} A_i$$

proving that

$$B^I\subseteq\prod_{i\in I} A_i \tag{2.58}$$

Further

$$\prod_{i\in I} A_i = \left\{f|f\in\left(\prod_{i\in I} A_i\right)^I\wedge\forall i\in I f(i)\in A_i\right\}\subseteq\left\{f|f\in\left(\prod_{i\in I} A_i\right)^I\right\} = \{f|f\in B^I\} = B^I$$

which combined with [eq: 2.58] proves that

$$B^I = \prod_{i\in I} A_i$$

□

Theorem 2.125. *Let I, J, B be classes, $f: I\rightarrow J$ a bijection and $\{A_j\}_{j\in J}$ then*

$$\beta:\prod_{j\in J} A_j\rightarrow\prod_{i\in I} A_{f(i)} \text{ where } \beta(x) = x\circ f$$

is a bijection.

Proof. First as $f: I\rightarrow J$ is a bijection, hence surjective, we have by [theorem: 2.102] that

$$\bigcup_{j\in J} A_j = \bigcup_{i\in I} A_{f(i)} \tag{2.59}$$

Let $x\in\prod_{j\in J}A_j$ then $x\in(\bigcup_{j\in J}A_j)^J$, which is equivalent with $x: J\rightarrow\bigcup_{j\in J}A_j$ is a function, and $\forall j\in J$ we have $x(j)\in A_j$. So $x\circ f: I\rightarrow\bigcup_{j\in J}A_j \underset{\text{[eq: 2.59]}}{=} \bigcup_{i\in I}A_{f(i)}$ is a function, proving that $x\circ f\in(\bigcup_{i\in I}A_{f(i)})^I$, further if $i\in I$ then $(x\circ f)(i)=x(f(i))\in A_{f(i)}$, hence

$$x\circ f\in\prod_{i\in I}A_{f(i)} \tag{2.60}$$

So

$$\beta: \prod_{j\in J}A_j\rightarrow\prod_{i\in I}A_{f(i)}$$

is indeed a function. To prove that it is a bijection note:

injectivity. Assume that $\beta(x)=\beta(y)$ then

$$\begin{aligned} x\circ f=y\circ f &\underset{f\text{ is bijective}}{\Rightarrow} (x\circ f)\circ f^{-1}=(y\circ f)\circ f^{-1}\\ &\Rightarrow x\circ(f\circ f^{-1})=y\circ(f\circ f^{-1})\\ &\Rightarrow x\circ\mathrm{Id}_J=y\circ\mathrm{Id}_J\\ &\Rightarrow x=y \end{aligned}$$

surjectivity. If $y\in\prod_{i\in I}A_{f(i)}$ then $y: I\rightarrow\bigcup_{i\in I}A_{f(i)} \underset{\text{[eq: 2.59]}}{=} \bigcup_{j\in J}A_j$ is a function and $\forall i\in I$ we have $y(i)\in A_{f(i)}$. As $f^{-1}: J\rightarrow I$ is a bijection we have that $y\circ f^{-1}: J\rightarrow\bigcup_{j\in J}A_j$ is a function, so that $y\circ f^{-1}\in(\bigcup_{j\in J}A_j)^J$, and $(y\circ f^{-1})(j)=y(f^{-1}(j))\in A_{f(f^{-1}(j))}=A_j$. So that

$$y\circ f^{-1}\in\prod_{j\in J}A_j$$

Finally $\beta(y\circ f^{-1})=(y\circ f^{-1})\circ f=y\circ(f^{-1}\circ f)=y\circ\mathrm{Id}_I=y$ proving surjectivity. □

Definition 2.126. *Let $\{A_i\}_{i\in I}\subseteq B$ be a family and $J\subseteq I$ then $\prod_{i\in J}A_i$ is the product based on the sub-family $\{A_i\}_{i\in J}\subseteq B$ [see definition: 2.92] or equivalently*

$$\prod_{i\in J}A_i=\left\{f: f\in\left(\bigcup_{i\in J}A_i\right)^J \text{ where } \forall i\in J \text{ we have } f(i)\in A_i\right\}$$

The following theorem will be used later in induction arguments.

Theorem 2.127. *Let $\{A_i\}_{i\in I}\subseteq B$, $i\in I$ and $b\in A_i$ then*

$$\text{if } x\in\prod_{j\in I\setminus\{i\}}A_j \text{ we have } y\in\prod_{i\in I}A_j$$

where y is defined by

$$y_j=y(j)=\begin{cases} b \text{ if } j=i\\ x_j \text{ if } j\in I\setminus\{i\}\end{cases} \underset{\text{def}}{=} \begin{cases} b \text{ if } j=i\\ x(j) \text{ if } j\in I\setminus\{i\}\end{cases}$$

Proof. If $x\in\prod_{j\in I\setminus\{i\}}A_j$ then $x\in\left(\bigcup_{j\in I\setminus\{i\}}A_i\right)^{I\setminus\{i\}}$ so that $x: I\setminus\{i\}\rightarrow\bigcup_{j\in I\setminus\{i\}}A_j$ is a function. As $i\notin(I\setminus\{i\})$, $I=(I\setminus\{i\})\bigcup\{i\}$ and $\bigcup_{j\in I}A_j \underset{\text{[theorem: 2.117]}}{=} A_i\bigcup\left(\bigcup_{j\in I\setminus\{i\}}A_j\right)$ we have by [theorem: 2.76] that

$$y: I\rightarrow\bigcup_{i\in I}A_i \text{ where } y(j)=\begin{cases} b \text{ if } j=i\\ x(j) \text{ if } j\in I\setminus\{i\}\end{cases}$$

is a function, so

$$y\in\left(\bigcup_{i\in I}A_i\right)^I \tag{2.61}$$

Further if $j\in I$ then either $j=i$ so that $y_j=y(i)=b\in A_i=A_j$ or $j\in I\setminus\{i\}$ then $y_j=y(j)=x(j)=x_j\in A_j$. Hence

$$\forall j\in I \text{ we have } y_j\in A_j \tag{2.62}$$

From [eq: 2.61] and [eq: 2.62] it follows by

$$y \in \prod_{i \in I} A_i$$

□

We introduce now the projection operator

Definition 2.128. *Let $\{A_i\}_{i \in I} \subseteq B$ be family then for $i \in I$ we define the projection function*

$$\pi_i: \prod_{j \in I} A_j \rightarrow A_i$$

where

$$\pi_i = \left\{ z | z = (x, x(i)) | x \in \prod_{j \in I} A_j \right\}$$

In other words $(x, y) \in \pi_i \Leftrightarrow x \in \prod_{j \in I} A_j$ and $y = x(i) \Leftrightarrow (i, y) \in x$

Proof. This definition only make sense if $\forall i \in I$ that $\pi_i: \prod_{j \in I} A_j \rightarrow A_i$ is a function. First if $(x, y) \in \pi_i$ we have that $x \in \prod_{j \in I} A_j$ and $y = x(i)$ giving $y \in A_i$, so $(x, y) \in (\prod_{i \in I} A_i) \times A_i$. Hence

$$\pi_i \subseteq \left(\prod_{i \in I} A_i \right) \times A_i \tag{2.63}$$

If $(x, y), (x, y') \in \pi_i$ then $y = x(i) \wedge y' = x(i)$ proving that $y = y'$ or

$$\pi_i: \prod_{j \in I} A_j \rightarrow A_i \text{ is a partial function}$$

If $x \in \prod_{j \in I} A_j$ then by definition $(x, x(i)) \in \pi_i$ proving that $x \in \operatorname{dom}(\pi_i)$ proving that $\prod_{j \in I} A_i \subseteq \operatorname{dom}(\pi_i)$, which by [theorem: 2.22] gives

$$\pi_i: \prod_{j \in I} A_j \rightarrow A_i \text{ is a function}$$

□

We are not yet finished with the product of a family of classes, however for some of the theorems we need the Axiom of Choice. For example to prove that the projection function is a surjection we need the Axiom of Choice.

Chapter 3
Relations

3.1 Relation

The idea of a relation is that we can specify which elements of a class are related to each other. You do this by specifying a class of pairs.

Definition 3.1. *Let A be a class then a relation in A is a sub-class of $A \times A$*

Notation 3.2. *So a relation is a set of pairs from elements of the same class, to avoid confusion with the graph of a function we use the following notation:*
If $R \subseteq A \times A$ is relation then instead of writing $(x, y) \in R$ we write $x R y$

Example 3.3. Let A be a class then $A \times A$ is a relation [as $A \times A \subseteq A \times A$]

We define now the following properties that a relation can have

Definition 3.4. *If A is a class and $R \subseteq A \times A$ a relation then we say that R is*

reflexive. *iff $\forall x \in A$ we have*

$$x R x$$

in other words every element is related to itself.

symmetric. *iff*

$$x R y \Rightarrow y R x$$

in other words if one element is related to a second element then the second element is related to the first element.

anti symmetric. *iff*

$$x R y \wedge y R x \Rightarrow x = y$$

in other words if on element is related to a second element and the second element is related to the first element then the two elements are the same.

transitive. *iff*

$$x R y \wedge y R z \Rightarrow x R z$$

in other words if one element is related to a second element and the second element is related to the third element then the first element is also related to the third element.

3.2 Equivalence relations

3.2.1 Equivalence relations and equivalence classes

Note that for classes and equality we have by [theorem: 1.8] that

- $A = A$
- $A = B \Rightarrow B = A$
- $A = B \wedge B = C \Rightarrow A = C$

If we want to create a relation that defines a kind of equality then it must behave in the same way as the equality for classes. This it he idea behind the following definition.

Definition 3.5. (Equivalence Relation) *If A is a class then a relation R is a* ***equivalence relation*** *iff it is reflexive, symmetric and transitive or in other words if*

reflectivity. $\forall x \in A\ x R x$

symetricity. $x R y \Rightarrow y R x$

transitivity. $x R y \wedge y R z \Rightarrow x R z$

Given a set A and a equivalence relation in A then it is useful to partition the set in subsets containing all the elements that are equivalent with each other. To do this we must first define what a partition of a set is.

Definition 3.6. *Let A be a set then a* ***partition*** *of A is a family $\{A_i\}_{i \in I} \subseteq \mathcal{P}(A)$ of non empty subsets of A [$\forall i \in I$ we have $A_i \neq \varnothing$] such that:*

1. $\bigcup_{i \in I} A_i = A$
2. $\forall i, j \in I$ *we have* $A_i \bigcap A_j = \varnothing \vee A_i = A_j$

Note 3.7. Condition (2) in the above definition is a weaker condition that pairwise disjointedness. For example if we define the family $(A_i)_{i \in \{1,2,3\}}$ by $A_1 = \{1\}$, $A_2 = \{1\}$ and $A_3 = \{2\}$ then this family is not pairwise disjoint as $1 \neq 2$ and $A_1 \bigcap A_2 \neq \varnothing$, however (2) is clearly satisfied.

We can also reformulate the definition of a partition of A in the following way

Theorem 3.8. *Let A be a set and $\{A_i\}_{i \in I} \subseteq \mathcal{P}(A)$ a family of non empty subsets of A then we have the following equivalences*

1. $\{A_i\}_{i \in I} \subseteq \mathcal{P}(A)$ *is a partition of A*
2. $\{A_i\}_{i \in I} \subseteq \mathcal{P}(A)$ *satisfies*
   a. $\forall x \in A$ *there exists a* $i \in I$ *such that* $x \in A_i$
   b. $\forall i, j \in I$ *with* $A_i \bigcap A_j \neq \varnothing$ *we have* $A_i = A_j$
3. $\{A_i\}_{i \in I} \subseteq \mathcal{P}(A)$ *satisfies*
   a. $\forall x \in A$ *there exists a* $i \in I$ *such that* $x \in A_i$
   b. $\forall i, j \in I$ *with* $A_i \neq A_j$ *we have* $A_i \bigcap A_j = \varnothing$

Proof.

$1 \Rightarrow 2$.

a) If $x \in A$ then as $A = \bigcup_{i \in I} A_i$ there exists a $i \in I$ such that $x \in A_i$

b) Let $i, j \in I$ with $A_i \bigcap A_j \neq \varnothing$. As by definition of a partition $A_i \bigcap A_j = \varnothing \vee A_i = A_j$ we must have that $A_i = A_j$.

$2 \Rightarrow 3$.

a) This is trivial

b) Let $i, j \in I$ with $A_i \neq A_j$. Assume that $A_i \bigcap A_j \neq \varnothing$ then by (2.b) we have $A_i = A_j$ contradicting $A_i = A_j$, so we must have that $A_i \bigcap A_j = \varnothing$

$3 \Rightarrow 1$.

a) Using (3.a) it follows that $A \subseteq \bigcup_{i \in I} A_i$. If $z \in \bigcup_{i \in I} A_i$ then there exists a $i \in I$ such that $x \in A_i$ [theorem: 2.101], hence as $A_i \in \mathcal{P}(A) \Rightarrow A_i \subseteq A$ it follows that $x \in A$, proving that $\bigcup_{i \in I} A_i \subseteq A$. So we have that

$$\bigcup_{i \in I} A_i = A$$

b) Let $i, j \in I$ then if $A_i \neq A_j$ we have by (3b) that $A_i \bigcap A_j = \varnothing$, so we have that $A_i = A_j \vee A_i \bigcap A_j = \varnothing$. □

We show now how a equivalence relation can be used to partition a set.

Definition 3.9. *Let A be a set and R a equivalence relation in A then given x we define the **equivalence class** of x noted by $R[x]$ by*

$$R[x] = \{y \in A | x R y\} \subseteq A$$

Note 3.10. Because $R[x] \subseteq A$ and A is a set we have by the axiom of subset 1.54 that $R[x]$ is a set.

We have the following important property for equivalence classes

Theorem 3.11. *Let A be a set with a equivalence relation R in A then*

1. $\forall x \in A$ *we have* $x \in R[x]$
2. $\forall x, y \in A$ *we have*
$$x R y \Leftrightarrow R[x] = R[y]$$
3. $\forall x \in A$ *we have*
$$y \in R[x] \Leftrightarrow R[x] = R[y]$$

Proof.

1. If $x \in A$ then using reflexivity we have $x R x$ so that $x \in R[x]$
2.
   ⇒. Let $z \in R[x]$ then $x R z$, further from $x R y$ we have $y R x$, so using transitivity it follows that $y R z$ or $z \in R[y]$. If $z \in R[y]$ then $y R z$ so as $x R y$ we have by transitivity that $x R z$ or that $z \in R$.

   ⇐. Using (1) $x \in R[x] \underset{R[x]=R[y]}{\Rightarrow} x \in R[y]$ proving that $r R y$
3.
   ⇒. If $y \in R[x]$ then $y R x$ hence by (2) $R[x] = R[y]$

   ⇐. If $R[x] = R[y]$ then $y R x$ proving that $y \in R[x]$ □

We define now a function that maps a element of as set on its equivalence class and use it to define a family of equivalence classes indexed by the elements of the set.

Definition 3.12. *Let A be a set and R a equivalence relation in A then $\{R[x]\}_{x \in A} \subseteq \mathcal{P}(X)$ is the family defined by the function $R[]: A \rightarrow \mathcal{P}(A)$ where $R[](x) = R[x]$*

Note 3.13. As $x \in R[x]$ we have that $\{R[x]\}_{x \in A}$ is a non empty family of subsets of A

Proof. We must of course prove that this a function. First $R[x]$ is defined for every $x \in A$ and calculates a unique set, further $R[x] \subseteq A \Rightarrow R[x] \in \mathcal{P}(A)$. So by [proposition: 2.86] $R[]: A \rightarrow \mathcal{P}[A]$ is a function. □

Theorem 3.14. *Let A be a set and R a equivalence relation in A then $\{R[x]\}_{x \in A}$ is a partition of A*

Proof. We use [theorem: 3.8] to prove this

1. If $x \in A$ then by [theorem: 3.11] we have that $x \in R[x]$ so that $x \in \bigcup_{x \in A} R[x]$
2. Let $x, y \in A$ such that $R[x] \bigcap R[y] \neq \varnothing$ then there exists a
$$z \in R[x] \bigcap R[y] \Rightarrow z R x \wedge z R y \underset{\text{symmetry}}{\Rightarrow} x R z \wedge z R y \underset{\text{transitivity}}{\Rightarrow} x R y$$

Using the above together with [theorem: 3.11] we have then that $R[x] = R[y]$

So by [theorem: 3.8] it follows that $\{R[x]\}_{x \in A} \subseteq \mathcal{P}(A)$ is a partition of A □

We have also the opposite of the above theorem in that a partition defines a equivalence relation that generates the same partition.

Theorem 3.15. *Let A be a set and $\{A_i\}_{i \in I} \subseteq \mathcal{P}(A)$ a partition of A. Define $R \subseteq A \times A$ by*

$$R = \{(x, y) | \exists i \in I \text{ such that } x \in A_i \wedge y \in A_i\}$$

then we have:

1. *R is a equivalence relation*
2. *$\forall i \in I$ there exists a $x \in A$ such that $R[x] = A_i$*
3. *$\forall x \in A$ there exists a $i \in I$ such that $R[x] = A_i$*

we call R is the called the ***equivalence relation associated with the partition*** $\{A_i\}_{i \in I} \subseteq \mathcal{P}(A)$

Proof.

1. We have:
   a. If $x \in A = \bigcup_{i \in I} A_i$ then $\exists i \in I$ such that $x \in A_i$ so that $(x, x) \in R$ or $x R x$
   b. If $x R y$ or $(x, y) \in R$ then $\exists i \in I$ such that $x \in A_i \wedge y \in A_i \Rightarrow y \in A_i \wedge x \in A_i$. Hence $(y, x) \in R$ or $y R x$.
   c. If $x R y \wedge y R z$ then $\exists i \in I$ such that $x, y \in A_i$ and $\exists j \in I$ such that $y, z \in A_j$. So $y \in A_i \bigcap A_j$ or $A_i \bigcap A_j \neq \varnothing$, by [theorem: 3.8] we have that $A_i = A_j$, hence $x, z \in A_i$ proving that $(x, z) \in R$ or $x R z$.
2. If $i \in I$ then as $A_i \neq \varnothing$ [a partition is a family of non empty subsets] there exists a $x \in A_i$. Take $y \in A_i$ then $x, y \in A_i$ or $y R x$ proving that $y \in R[x]$. So

   $$A_i \subseteq R[x]$$

   Take $y \in R[x]$ then $y R x$ so there exist a $j \in I$ such that $x, y \in A_j$, hence $A_i \bigcap A_j \neq \varnothing$ which by [theorem: 3.8] proves that $A_i = A_j$, so that $y \in A_i$. So $R[x] \subseteq A_i$ giving

   $$A_i = R[x]$$
3. If $x \in A$ then $\exists i \in I$ such that $x \in A_i$. Take $y \in A_i$ then $x, y \in A_i$ or $y R x$ proving that $y \in R[x]$, hence

   $$A_i \subseteq R[x]$$

   Take $y \in R[x]$ then $y R x$ so there exist a $j \in I$ such that $x, y \in A_j$, hence $A_i \bigcap A_j \neq \varnothing$ which by [theorem: 3.8] proves that $A_i = A_j$, so that $y \in A_i$. So $R[x] \subseteq A_i$ giving

   $$A_i = R[x]$$

□

Definition 3.16. *Let A be a set and R a relation then A / R is defined by*

$$A / R = \{R[x] | x \in A\}$$

Note 3.17. As $\forall x \in X$ $R[x] \in \mathcal{P}(A)$ it follows that

$$R / X \in \mathcal{P}(A).$$

As A is a set it follows from the Axiom Power [axiom: 1.64] that $P(A)$ is a set, applying the Axiom of Subsets [axiom: 1.54] we have

$$R / X \text{ is a set}$$

3.2.2 Functions and equivalence relations

In this section we show how a function can be decomposed as the composition of a surjection, a bijection and injection. First we examine the relation between functions and equivalence relations.

We can use functions to generate a equivalence relation on the domain of the function based on a equivalence relation on the target of the function.

Theorem 3.18. *$f: A \rightarrow B$ a function and R a equivalence relation in A then*

$$f\langle R\rangle = \{(x, y) | f(x)\, R\, f(y)\} \subseteq A \times A$$

is a equivalence relation in A

Proof.

reflectivity. If $x \in A$ then $f(x) \in B$ so that $f(x)\, R\, f(x)$ hence by definition $x\, R x$

symmetric. If $x\, R y$ then $f(x)\, R\, f(y)$ so that $f(y)\, R\, f(x)$ proving $y\, R x$

transitivity. If $x\, R y \wedge y\, R z$ then $f(x)\, R\, f(y) \wedge f(y)\, R\, f(z)$ so that $f(x)\, R\, f(x)$ proving that $x\, R z$. □

A equivalence relation on a set induce a equivalence relation on a subset

Theorem 3.19. *Let A be a class, $B \subseteq A$ a sub-class and R a equivalence relation in R then $R_{|B}$ defined by*

$$R_{|B} = \{(x, y) | x \in B \wedge y \in B \wedge x\, R y\} = R \bigcap (B \times B)$$

is a equivalence relation.

Proof.

reflexivity. If $x \in B$ then $x\, R x$ so that $x\, R_{|B}\, x$

symmetric. If $x\, R_{|B} y \Rightarrow x \in B \wedge y \in B \wedge \mathrm{xRy} \Rightarrow \mathrm{yR}_{|B} x$

transitivity. If $x\, R_{|B}\, y \wedge y R_{|B}\, z$ then $x, y, z \in \mathbb{R}$ and $x\, R y \wedge y\, R z$ so that $x, z \in B$ and $x\, R z$ proving $x\, R_{|B}\, z$ □

Theorem 3.20. *If $f: A \rightarrow B$ is a function then R_f defined by*

$$R_f = \{(x, y) \in A \times A | f(x) = f(y)\}$$

is a relation. R_f is called the ***equivalence relation determined by f***

Proof.

reflexivity. If $x \in A$ then $f(x) = f(x)$ proving that $x\, R_f\, x$

symmetric. If $x\, R_f y$ then $f(x) = f(y) \Rightarrow f(y) = f(x)$ proving that $y R_f\, x$

transitivity. If $x\, R_f\, y \wedge y R_f\, x$ then $f(x) = f(y)$ and $f(y) = f(z)$ so that $f(x) = f(x)$ hence $x\, R_f\, z$ □

We can also do the opposite and associate a function with a equivalence relation

Theorem 3.21. (Canonical Function) *Let A be a set and R a equivalence relation in A then:*

1. *$f_R: A \rightarrow A / R$ defined by $f_R(x) = R[x]$ is a surjective function.*
2. *$R_{R_f} = R$*

$f_R: A \rightarrow A / R$ is called the **Canonical function associated with R**

Proof.

1. As for every $x \in A$ we have the unique $R[x] \in R / X$ it follows from [proposition: 2.86] that

$$f_R: A \rightarrow A / R \text{ is a function}$$

Let $y \in R/X$ then $\exists x \in A$ such that $y = R[x]$ so that $(x, y) = (x, R[x]) \in f_R$ proving that $y \in \text{range}(f_R)$. So $R/X \subseteq \text{range}(f_R)$ which by [theorem: 2.47] proves that

$$f_R: A \rightarrow A/R \text{ is surjective}$$

2. We have

$$\begin{array}{rcl} (x, y) \in R & \Leftrightarrow & x\,R\,y \\ & \underset{\text{[theorem: 3.11]}}{\Leftrightarrow} & R[x] = R[y] \\ & \Leftrightarrow & f_R(x) = f_R(y) \\ & \Leftrightarrow & (x, y) \in R_{f_R} \end{array}$$

□

We use the above to decompose every function as the composition of a surjection, bijection and injection.

Theorem 3.22. *Let A, B be sets and $f: A \rightarrow B$ a function and define the following functions:*

a) $s_f: A/R_f \rightarrow f(A)$ *where* $s_f = \{(R_f[x], f(x)) | x \in A\}$

b) $i_{f(A)}: f(A) \rightarrow B$ *where* $i_{f(A)} = \{(x, x) | x \in f(A)\}$ *[the inclusion function see [example: 2.49]*

c) $f_{R_f}: A \rightarrow A/R_f$ *where* $f_{R_f}(x) = R_f[x]$ *[theorem: 3.21]*

then

1. $s_f: A/R_f \rightarrow f(A)$ *is a bijection*
2. $i_{f(A)}: f(A) \rightarrow B$ *is a injective function*
3. $f_{R_f}: A \rightarrow A/R_f$ *is a surjective function*
4. $f = i_{f(A)} \circ (s_f \circ f_{R_f}) \underset{\text{[theorem: 2.18]}}{=} (i_{f(A)} \circ s_f) \circ f_{R_f}$

Proof. Using [example: 2.49] and [theorem: 3.21] we have that

$$i_{f(A)}: f(A) \rightarrow B \text{ is a injective function}$$

and

$$f_{R_f}: A \rightarrow A/R_f \text{ is surjective function}$$

We proceed now to prove that s_f is a bijection. If $(x, y) \in s_f$ then there exists a $a \in A$ such that $(x, y) = (R_f[a], f(a))$ hence $x = R_f[a] \in A/R_f$ and $y = f(a) \Rightarrow (a, y) \in f \Rightarrow y \in f(A)$. So that $(x, y) \in (A/R_f) \times f(A)$ or

$$s_f \subseteq (A/R_f) \times f(A)$$

If $(x, y), (x, y') \in s_f$ then there exists $a, a' \in A$ such that

$$(x, y) = (R_f[a], f(a)) \wedge (x, y') = (R_f[a'], f(a'))$$

or

$$x = R_f[a] \wedge y = f(a) \wedge x = R_f[a'] \wedge y' = f(a') \tag{3.1}$$

From the above $R_f[a] = x = R_f[a']$, which using [theorem: 3.11] means that $a\,R_f\,a'$, so by the definition of R_f [theorem: 3.20] we have $f(a) = f(a')$. As by [eq: 3.1] $y = f(a) \wedge y' = f(a')$ it follows that $y = y'$. So

$$s_f: A/R_f \rightarrow f(A) \text{ is a partial function}$$

If $x \in A/R_f$ then $\exists a \in A$ such that $x = [a]$, hence if we take $y = f(A)$ we have that $(x, y) = ([a], f(a)) \in s_f$ proving that $x \in \text{dom}(s_f)$. So $A/R_f \subseteq \text{dom}(f)$ which by [proposition: 2.22] proves that

$$s_f: A/R_f \rightarrow f(A) \text{ is a function}$$

Let $(x,y),(x',y)\in s_f$ then $\exists a,a'\in A$ such that $(x,y)=(R_f[a],f(a))$ and $(x',y)=(R_f[a'],f(a'))$, hence

$$x=R_f[a]\wedge x'=R_f[a']\wedge y=f(a)\wedge y=f(a') \tag{3.2}$$

From $f(a)=y=f(a')$ it follows that $f(a)=f(a')$, which by the definition of R_f [theorem: 3.20] proves that $a\,R_f\,a'$. Using [theorem: 3.11 it follows that $R_f[a]=R_f[a']$ or using [eq: 3.2] that $x=x'$. So we have proved that

$$s_f\colon A/R_f\rightarrow f(A)\text{ is injective} \tag{3.3}$$

Let $y\in f(A)$ then there exist a $a\in A$ such that $(a,y)\in f\Rightarrow y=f(a)$. But then $(R_f[a],y)=(R_f[a],f(a))\in s_f$ proving that $y\in\text{range}(s_f)$. So $A/R_f\subseteq\text{range}(s_f)$ which by [proposition: 2.47] proves that

$$s_f\colon A/R_f\rightarrow f(A)\text{ is surjective} \tag{3.4}$$

Combining [eq: 3.3] and [eq: 3.4] it follows that

$$s_f\colon A/R_f\rightarrow f(A)\text{ is a bijection}$$

Now we proceed to prove that $f=(i_{f(A)}\circ s_f)\circ f_{R_f}$. Let $(x,u)\in(i_{f(A)}\circ s_f)\circ f_{R_f}$ then $\exists y$ such that $(x,y)\in f_{R_f}\wedge(y,u)\in i_{f(A)}\circ s_f$, from $(y,u)\in i_{f(A)}\circ s_f$ $\exists$z such that $(y,z)\in s_f\wedge(z,u)\in i_{f(A)}$, summarized

$$(x,y)\in f_{R_f}\wedge(y,z)\in s_f\wedge(z,u)\in i_{f(A)} \tag{3.5}$$

From $(x,y)\in f_{R_f}$ it follows that $\exists a\in A$ such that $(x,y)=(a,R_f[a])$ or

$$x=a\wedge y=R_f[a] \tag{3.6}$$

From $(y,z)\in s_f$ it follows that $\exists a'\in A$ such that $(y,z)=(R_f[a'],f(a'))$ or $y=R_f[a']\wedge z=f(a')$. As $y\underset{\text{[eq: 3.6]}}{=}R_f[a]$ we have that $R_f[a]=R_f[a']$, which by [theorem: 3.11] proves that $a\,R_f\,a'$, so by the definition of R_f we have $f(a)=f(a')$ hence $z=f(a)$. From $(z,u)\in i_{f(A)}$ it follows that $z=u$ hence $u=f(a)$. As $x\underset{\text{[eq: 3.6]}}{=}a$ it follows that $(x,u)=(a,f(a))\in f$. Hence

$$(i_{f(A)}\circ s_f)\circ f_{R_f}\subseteq f \tag{3.7}$$

Finally if $(x,y)\in f$ then as $f\subseteq A\times B$ proves that $x\in A$ and $f(x)=y\in f(A)$. Hence $(R_f[x],f(x))\in s_f$, $(x,R_f[x])\in f_{R_f}$ and $(f(x),y)=(f(x),f(x))\in i_{f(A)}$. So that $(R_f[x],y)\in i_{f(A)}\circ s_f$ and $(x,R_f[x])\in f_{R_f}$ proving that $(x,y)\in(i_{f(A)}\circ s_f)\circ f_{R_f}$. So $f\subseteq(i_{f(A)}\circ s_f)\circ f_{R_f}$ which combined with [eq: 3.7] gives

$$f=(i_{f(A)}\circ s_f)\circ f_{R_f}$$ □

Notation 3.23. *For the rest of this book we use the standard convention of noting a equivalence relation as $\sim$, The definition of $\sim$ should then be clear from the context. If many equivalence relations are used in the same context we use superscripts like $\sim_{\mathbb{R}}$ and $\sim_{\mathbb{Z}}$ to avoid conflicts.*

3.3 Partial ordered classes

3.3.1 Order relation

First we define a partial order relation that allows us to compare two elements and specify which element 'lies before' another element.

Definition 3.24. (Pre-order) *Let A be a class then a relation $R\subseteq A\times A$ in A is a pre-order if it is **reflexive** and **transitive** or in other words:*

reflectivity. *$\forall x\in A$ we have $x\,R\,x$*

transitivity. *If $x R y \wedge y R z$ then $x R z$*

Definition 3.25. *$\langle A, R\rangle$ is a pre-ordered class iff A is a class and R is a pre-order in A*

A order relation is a pre-order with one extra condition

Definition 3.26. (Order relation) *If A is a class then a relation $R \subseteq A \times A$ in A is a **order** if it is a pre-order that is anti-symmetric or in other words:*

reflectivity. *$\forall x \in A$ we have $x R x$*

anti-symmetry. *If $x R y \wedge y R x$ then $x = y$*

transitive. *If $x R y \wedge y R z$ then $x R z$*

Definition 3.27. (Partial ordered class) *$\langle A, R\rangle$ is a **partial ordered class** if A is a class and R is a order.*

Notation 3.28. *We use the standard convention of noting a pre-order relation as $\leqslant$, The definition of $\leqslant$ should then be clear from the context. If many pre-order relations are used in the same context we use superscripts like $\leqslant_{\mathbb{R}}$ and $\leqslant_{\mathbb{Z}}$ or $\preccurlyeq$ to avoid conflicts.*

Definition 3.29. *If $\langle A, \leqslant\rangle$ is a pre-ordered or partial class and $x, y, z \in A$ then we define:*

$$\begin{array}{lll} x \leqslant y \leqslant z & \text{is the same as} & x \leqslant y \wedge y \leqslant z \\ x \leqslant y < z & \text{is the same as} & x \leqslant y \wedge y < z \\ x < y \leqslant z & \text{is the same as} & x < y \wedge y \leqslant z \\ x < y < z & \text{is the same as} & x < y \wedge y < z \end{array}$$

Definition 3.30. *If $\langle A, \leqslant\rangle$ is a pre-ordered class [or partial ordered class] then $x < y$ is equivalent with $x \leqslant y \wedge x \neq y$*

Theorem 3.31. *If $\langle A, \leqslant\rangle$ is a partially ordered set then*

1. $x \leqslant y \wedge y < z \Rightarrow x < z$
2. $x < y \wedge y \leqslant z \Rightarrow x < z$
3. $x < y \wedge y < z \Rightarrow x < z$
4. $(x < y \vee x = y) \Leftrightarrow (x \leqslant y)$

or in other words

1. $x \leqslant y < z \Rightarrow x < z$
2. $x < y \leqslant z \Rightarrow x < z$
3. $x < y < z \Rightarrow x < z$
4. $(x < y \vee x = y) \Leftrightarrow x \leqslant y$

Proof.

1. If $x \leqslant y \wedge y < z$ then $x \leqslant y \wedge y \leqslant z \wedge y \neq z$, so that $x \leqslant z$ and $y \neq z$. Assume that $x = z$ then $z \leqslant y \underset{y \leqslant z}{=} z = y$ contradicting $y \neq z$, so we must have $x \neq z$, which together with $x \leqslant z$ gives

$$x < z$$

2. If $x < y \wedge y \leqslant z$ then $x \leqslant y \wedge y \leqslant z \wedge x \neq y$, so that $x \leqslant z$ and $x \neq y$. Assume that $x = z$ then $y \leqslant x \underset{x \leqslant y}{\Rightarrow} y = x$ contradicting $x \neq y$, so we must have $x \neq z$, which together with $x \leqslant z$ gives

$$x < z$$

3. If $x < y \wedge y < z$ then $x \neq y \wedge x \leqslant y \wedge y < z$ so that by (1) we have $x < z$

4. We have

$$\begin{aligned}(x<y\vee x=y) &\Leftrightarrow ((x\leqslant y\wedge x\neq y)\vee x=y)\\ &\Leftrightarrow ((x\leqslant y\vee x=y)\wedge(x\neq y\vee x=y))\\ &\Leftrightarrow x\leqslant y\vee x=y\\ &\Leftrightarrow x\leqslant y\end{aligned}$$

□

Example 3.32. Let A be a class of classes and $\leqslant$ defined by $\leqslant=\{(x,y)\in\mathcal{A}\times\mathcal{A}|x\subseteq y\}$ then $\langle\mathcal{A},\leqslant\rangle$ is a partial ordered class

Proof.

reflectivity. If $A\in\mathcal{C}$ then by [theorem: 1.8] $A\subseteq A$ so that $A\leqslant A$

anti-symmetric. If $A\leqslant B$ and $B\leqslant A$ then $A\subseteq B\wedge B\subseteq A$ so that by [theorem: 1.8] $A=B$

transitivity. If $A\leqslant B\wedge B\leqslant C$ then $A\subseteq B\wedge B\subseteq C$ so that by [theorem: 1.8] $A\subseteq C$ or $A\leqslant C$ □

Every pre-order can be used as the base to create a order relation as is expressed in the following theorem. The basic idea is that $x\leqslant y\wedge y\leqslant x\Rightarrow x=y$ is missing from a pre-order. By defining a equivalence relation $\sim$ such that $x\sim y$ if $x\leqslant y\wedge y\leqslant x$ we turn this in equality of equivalence classes. This is a typical example about the use of equivalence relations, they allow you to define a new type of equality, so that objects that are not equal have associated equivalence classes that are equal.

Theorem 3.33. *Let $\langle A,\leqslant\rangle$ be a pre-ordered set then we have*

1. $\sim\subseteq A\times A$ *defined by* $\sim=\{(x,y)\in A|x\leqslant y\wedge y\leqslant x\}$ *is a equivalence relation*
2. *Define* $\preccurlyeq\subseteq(A/\sim)\times(A/\sim)$ *by*

$$\preccurlyeq=\{(x,y)\in(A/\sim)\times(A/\sim)|\exists x'\in\sim[x] \textit{ and } \exists y'\in\sim[y] \textit{ such that } x'\leqslant y'\}$$

then $\preccurlyeq$ *is a order relation in* $A/\sim$. *So* $\langle A/\sim,\preccurlyeq\rangle$ *is a partial ordered set*

3. $\forall x,y\in A$ *we have* $x\leqslant y\Leftrightarrow\sim[x]\preccurlyeq\sim[y]$

Proof.

1. To prove that $\sim$ is a equivalence relation note:

   reflectivity. If $x\in A$ then $x\leqslant x$ proving that $x\sim x$

   symmetric. If $x\sim y$ then $x\leqslant y\wedge y\leqslant x\Rightarrow y\leqslant x\wedge x\leqslant y$ so that $y\sim x$

   transitive. If $x\sim y$ and $y\sim z$ then $x\leqslant y\wedge y\leqslant x\wedge y\leqslant z\wedge z\leqslant y$ so that $x\leqslant z$ and $z\leqslant x$ or $x\sim z$

2. To prove that $\preccurlyeq$ is a order relation we must prove reflectivity, symmetry and transitivity:

   reflexivity. Take $\sim[x]$ then as $x\leqslant x$ there exists a $u\in\sim[x]$ and $v\in\sim[x]$ such that $u\leqslant v$ [just take $u=x=v$] so that

$$\sim[x]\preccurlyeq\sim[x]$$

   symmetry. Let $\sim[x]\leqslant\sim[y]$ and $\sim[y]\leqslant\sim[x]$ then $\exists x',x''\in\sim[x]$, $\exists y'y''\in\sim[y]$ such that

$$x'\leqslant y'\wedge y''\leqslant x''$$

   From $\exists x',x''\in\sim[x]$, $\exists y'y''\in\sim[y]$ we have

$$x'\leqslant x\wedge x\leqslant x'\wedge x''\leqslant x\wedge x\leqslant x''\wedge y'\leqslant y\wedge y\leqslant y'\wedge y''\leqslant y\wedge y\leqslant y''$$

   From $x\leqslant x'$ and $x'\leqslant y'$ we have $x\leqslant y'$, as $y'\leqslant y$ we have

$$x\leqslant y$$

From $y \leqslant y''$ and $y'' \leqslant x''$ we have $y \leqslant x''$, as $x'' \leqslant x$ it follows that

$$y \leqslant x$$

Finally from $x \leqslant y$ and $y \leqslant x$ we have that $x \sim y$ which by [theorem: 3.11] gives

$$\sim[x] = \sim[y]$$

transitivity. Assume that $\sim[x] \preccurlyeq \sim[y]$ and $\sim[y] \preccurlyeq \sim[z]$ then we have the existence of $x' \in \sim[x]$, $y', y'' \in \sim[y]$ and $z' \in \sim[z]$ such that

$$x' \leqslant y' \wedge y'' \leqslant z'$$

From $x' \in \sim[x]$, $y', y'' \in \sim[y]$ and $z' \in \sim[z]$ it follows that

$$x' \leqslant x \wedge x \leqslant x' \wedge y' \leqslant y \wedge y \leqslant y' \wedge y'' \leqslant y \wedge y \leqslant y'' \wedge z' \leqslant z \wedge z \leqslant z'$$

From $x \leqslant x'$ and $x' \leqslant y'$ we have $x \leqslant y'$, as $y' \leqslant y$ we have $x \leqslant y$, as $y \leqslant y''$ it follows that $x \leqslant y''$, from $y'' \leqslant z'$ we have that $x \leqslant z'$ and finally from $z' \leqslant z$ it follows that $x \leqslant z$. Hence

$$\sim[x] \preccurlyeq \sim[z]$$

3.

$\Rightarrow$. If $x \leqslant y$ then as $x \in \sim[x]$ and $y \in \sim[y]$ we have $\sim[x] \preccurlyeq \sim[y]$

$\Leftarrow$. If $\sim[x] \preccurlyeq \sim[y]$ then $\exists x' \in \sim[x]$ and $\exists y' \in \sim[y]$ such that

$$x' \leqslant y'$$

From $x' \in \sim[x]$ and $y' \in \sim[y]$ we have that

$$x' \leqslant x \wedge x \leqslant x' \wedge y' \leqslant y \wedge y \leqslant y'$$

From $x \leqslant x'$ and $x' \leqslant y'$ it follows that $x \leqslant y'$ and as $y' \leqslant y$ it follows that

$$x \leqslant y$$

□

Given a partial ordered class then we can induce the order on a sub-class making the sub-class also a partial ordered class.

Theorem 3.34. *If $\langle A, \leqslant \rangle$ is a partial ordered sets and $B \subseteq A$ then $\leqslant_{|B}$ defined by*

$$\leqslant_{|B} = \leqslant \bigcap B \times B = B$$

is a order relation in B making $\langle B, \leqslant_{|B} \rangle$ a partial ordered set.

Proof.

reflectivity. If $x \in B$ then $x \leqslant x$ or $(x, x) \in \leqslant \underset{x \in B}{\Rightarrow} (x, x) \in \leqslant \bigcap (B \times B)$ hence $x \leqslant_{|B} y$

symmetry. If $x \leqslant_{|B} y \wedge y \leqslant_{|B} x \Rightarrow x \leqslant y \wedge y \leqslant x \Rightarrow x = y$

transitivity. If $x \leqslant_{|B} y \wedge y \leqslant_{|B} z \Rightarrow x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z \underset{x,z \in B}{\Rightarrow} x \leqslant_{|B} z$ □

The following shows a technique of defining a partial order on the Cartesian product of partial ordered set.

Theorem 3.35. **(Lexical ordering)** *Let $\langle A, \leqslant_A \rangle$ and $\langle B, \leqslant_B \rangle$ be partial ordered classes then $\leqslant_{A \times B}$ defined by*

$$\leqslant_{A \times B} = \{((x, y), (u, v)) \in (A \times B) \times (A \times B) | (x \neq u \wedge x \leqslant_A u) \vee (x = y \wedge y \leqslant_B v\}$$

is a order in $A \times B$ making $\langle (A \times B) \times (A \times B), \leqslant_{A \times B} \rangle$ a partial ordered set

Proof.

reflexivity. If $(x, y) \in A \times B$ then $x \leqslant_A x \wedge y \leqslant_B y$ proving that $(x, y) \leqslant_{A \times B} (x, y)$

symmetry. Let $(x, y) \leqslant_{A \times B} (u, v) \wedge (u, v) \leqslant_{A \times B} (x, y)$. If $x \neq u$ we would have $x \leqslant_A u \wedge u \leqslant_A x \Rightarrow x = u$ a contradiction. So we must have that $x = u$ but then $y \leqslant_B v \wedge v \leqslant_{|B} y \Rightarrow y = v$ proving that

$$(x, y) = (u, v)$$

transitivity. Let $(x, y) \leqslant_{A \times B} (u, v) \wedge (u, v) \leqslant_{A \times B} (r, s)$ then we have to consider the following cases:

$x = u$. Then $y \leqslant_B v$ and we have the following possibilities

$u = r$. Then $v \leqslant_B s$ so that $y \leqslant_B s$ which as $x = r$ proves that

$$(x, y) \leqslant_{A \times B} (r, s)$$

$u \neq r$. Then $u \leqslant_A r \underset{x=u}{\Rightarrow} x \leqslant_A r$ which as $x \neq r$ proves that

$$(x, y) \leqslant_{A \times B} (r, s)$$

$x \neq u$. Then $x \leqslant_A u$ and we have the following possibilities

$u = r$. Then $x \leqslant_A u \underset{u=r}{\Rightarrow} x \leqslant_A r$ and $x \neq r$ so that

$$(x, y) \leqslant_{A \times B} (r, s)$$

$u \neq r$. Then $u \leqslant_A r$ so that $x \leqslant_A r$. If $x = r$ then we would have $x \leqslant_A u \wedge u \leqslant_A x$ giving $x = u$ contradicting $x \neq u$. So we must have $x \neq r$ which as $x \leqslant_A r$ gives

$$(x, y) \leqslant_{A \times B} (r, s)$$

□

Definition 3.36. *Let $\langle A, \leqslant \rangle$ be a partial ordered class then $x, y \in A$ are **comparable** if $x \leqslant y$ or $y \leqslant x$*

Theorem 3.37. *Let $\langle A, \leqslant \rangle$ be a partial ordered class and $x, y \in A$ comparable elements then we have either $x \leqslant y$ or $y < x$*

Proof. As x, y are comparable then we have $x \leqslant y \vee y \leqslant x$, consider the following cases:

$x \leqslant y$. hen $x \leqslant y$

$\neg(x \leqslant y)$. then we must have $y \leqslant x$. If $x = y$ then as $x \leqslant x$ we have $x \leqslant y$ contradicting $\neg(x \leqslant y)$ so that $x \neq y$ proving $y < x$.

Hence we have

$$x \leqslant y \vee y < x$$

□

Definition 3.38. *A pre-ordered class $\langle A, \leqslant \rangle$ is a **totally ordered class** iff*

$$\forall x, y \in A \text{ we have } x \leqslant y \vee y \leqslant x$$

*In other words $\langle A, \leqslant \rangle$ is a **totally ordered class** if every pair of elements are comparable. Other names used in the literature are **fully ordered class** or **linear ordered class**.*

Definition 3.39. (chain) *Let $\langle A, \leqslant \rangle$ be a partial ordered class and $C \subseteq A$ then C is called a **chain** if $\forall x, y \in C$ we have that $x \leqslant y$ or $y \leqslant x$.*

Example 3.40. Let $\langle A, \leqslant \rangle$ be a partial ordered class then $\varnothing$ is a chain

Proof. The condition $\forall x, y \in \varnothing$ we have that x, y are comparable is satisfied vacuously. □

Theorem 3.41. *Let $\langle A, \leqslant \rangle$ be a partial ordered class and $B \subseteq A$ a chain then $\langle B, \leqslant_{|B} \rangle$ is a totally ordered class*

Proof. Using [theorem: 3.34] we have that $\langle B, \leqslant_{|B} \rangle$ is a partial ordered class. Let $x, y \in B$ then as B is a chain we have that $\forall x, y \in B\ x \leqslant y \vee y \leqslant x$ or using the definition of $\leqslant_{|B}$ that $x \leqslant_{|B} y \vee y \leqslant_{|B} x$. □

Theorem 3.42. *Let $\langle A, \leqslant \rangle$ be a totally ordered class and $B \subseteq A$ then B is a chain [hence by [theorem: 3.41] $\langle B, \leqslant_{|B} \rangle$ is a totally ordered class]*

Proof. If $x, y \in B$ then $x, y \in A$ and as A is totally ordered we have $x \leqslant y \vee y \leqslant x$ so B is a chain □

Theorem 3.43. *Let $\langle A, \leqslant_A \rangle$ and $\langle B, \leqslant_B \rangle$ be totally ordered classes then $\langle A \times B, \leqslant_{A \times B} \rangle$ is a totally ordered class.*

Proof. First $\langle A \times B, \leqslant_{A \times B} \rangle$ is a partially ordered class by [theorem: 3.35]. If $(x, y), (x', y') \in A \times B$ then we have for x, x' either

- **$x = x'$.** As $\langle B, \leqslant_B \rangle$ is fully ordered we have either
  - **$y \leqslant y'$.** then $(x, y) \leqslant (x', y')$
  - **$y' \leqslant y$.** then $(x', y') \leqslant (x, y)$
- **$x \neq x'$.** As $\langle A, \leqslant_A \rangle$ is fully ordered we have either
  - **$x \leqslant x'$.** then $(x, y) \leqslant (x', y')$
  - **$x' \leqslant x$.** then $(x', y') \leqslant (x, y)$ □

Definition 3.44. (Initial Segment) *If $\langle A, \leqslant \rangle$ is a partial ordered class, $a \in A$ then a* ***initial segment of A determined by a*** *noted as $S_{A,a}$ is defined by*

$$S_{A,a} = \{x \in A | x < a\}$$

We have the following trivial result for initial segments.

Proposition 3.45. *If $\langle A, \leqslant \rangle$ is a partial ordered class and $a, b \in A$ such that $a \leqslant b$ then $S_{A,a} \subseteq S_{A,b}$*

Proof. If $x \in S_{A,a}$ then $x < a \underset{a \leqslant b}{\Rightarrow} x < b$ proving that $x \in S_{A,b}$ □

Theorem 3.46. *If $\langle A, \leqslant \rangle$ is a partial ordered class and P is a initial segment of A and Q is a initial segment of P [using the induced order $\leqslant_{|P}$] then A is a initial segment of A*

Proof. Using the hypothesis there exists $a \in A$ such that $P = \{x \in A | x < a\}$ and a $b \in P$ such that $Q = \{x \in P | x < b\}$. Consider then the initial segment $S_{A,b} = \{x \in A | x < b\}$ of A determined by a then we have

$$\begin{array}{rcl}
x \in S_{A,b} & \Rightarrow & x \in A \wedge x < b \\
 & \underset{b < a \Rightarrow x < b \Rightarrow x < a}{\Rightarrow} & x \in A \wedge x < a \wedge x < b \\
 & \Rightarrow & x \in P \wedge x < b \\
 & \Rightarrow & x \in P \wedge x <_{|P} b \\
 & \Rightarrow & x \in Q \\
x \in Q & \Rightarrow & x \in P \wedge x <_{|P} b \\
 & \Rightarrow & x \in P \wedge x < b \\
 & \underset{P \subseteq A}{\Rightarrow} & x \in A \wedge x < b \\
 & \Rightarrow & x \in S_{A,b}
\end{array}$$

Hence $Q = S_{A,b}$ a initial segment of A □

Next we define the concept of a Dedekind cut that will be used later to define the set of real numbers,

Definition 3.47. (Dedekind cut) *Let $\langle A, \leqslant \rangle$ be a partial ordered class a pair $\langle C, D \rangle$ is a **cut** of A iff*

1. $C, D \subseteq A$
2. $C \neq \varnothing \wedge D \neq \varnothing$
3. $C \bigcap D = \varnothing$
4. $x \in C \wedge y \leqslant x \Rightarrow y \in C$
5. $x \in D \wedge x \leqslant y \Rightarrow D$

3.3.2 Order relations and functions

Functions between two partial ordered classes can be classified based on the fact that they preserve or not preserve the order relation. This is expressed in the next definition.

Definition 3.48. *Let $\langle A, \leqslant_A \rangle$, $\langle B, \leqslant_B \rangle$ be partial ordered classes and $f: A \rightarrow B$ a function then:*

1. *$f: A \rightarrow B$ is **increasing** if $\forall x, y \in A$ with $x \leqslant y$ we have $f(x) \leqslant f(y)$. Another name that is used is **a order homeomorphism** [a homeomorphism is a function that preserver a certain operation, in this case the order relation]*
2. *$f: A \rightarrow B$ is **strictly increasing** if $\forall x, y \in A$ with $x < y$ we have $f(x) < f(y)$*
3. *$f: A \rightarrow B$ is **decreasing** if $\forall x, y \in A$ with $x \leqslant y$ we have $f(y) \leqslant f(x)$*
4. *$f: A \rightarrow B$ is **strictly decreasing** if $\forall x, y \in A$ with $x < y$ we have $f(y) < f(x)$*
5. *$f: A \rightarrow B$ is a **order isomorphism** if $\forall x, y \in A$ with $x \leqslant y \Leftrightarrow f(x) \leqslant f(y)$*

Definition 3.49. *Two partial classes $\langle A, \leqslant_A \rangle$ and $\langle B, \leqslant_B \rangle$ are **order isomorphic** noted as $A \cong B$ if there exists order isomorphism between A and B.*

Theorem 3.50. *Let $\langle A, \leqslant_A \rangle$, $\langle B, \leqslant_B \rangle, \langle C, \leqslant_C \rangle$ be partial ordered classes and $f: A \rightarrow B$, $g: B \rightarrow C$ functions then we have:*

1. *If $f: A \rightarrow B$ is increasing and $g: B \rightarrow C$ is increasing then $g \circ f: A \rightarrow C$ is increasing*
2. *If $f: A \rightarrow B$ is strictly increasing and $g: B \rightarrow C$ is strictly increasing then $g \circ f: A \rightarrow C$ is strictly increasing*
3. *If $f: A \rightarrow B$ is a order isomorphism and $g: B \rightarrow C$ is a order isomorphism then $g \circ f: A \rightarrow C$ is order isomorphism*

Proof.

1. Let $x, y \in A$ with $x \leqslant_A y$ then $f(x) \leqslant f_B(y)$ hence $(g \circ f)(x) = g(f(x)) \leqslant_C g(f(y)) = (g \circ f)()$.
2. Let $x, y \in A$ with $x <_A y$ then $f(x) <_B f(y)$ hence $(g \circ f)(x) = g(f(x)) <_C g(f(y)) = (g \circ f)()$.
3. Let $x, y \in A$. If $x \leqslant_A y$ then $f(x) \leqslant_B f(y)$ hence $(g \circ f)(x) = g(f(x)) \leqslant_C g(f(y)) = (g \circ f)(y)$. Also if $(g \circ f)(x) \leqslant_C (g \circ f)(y)$ then $g(f(x)) \leqslant_C g(f(y))$ so that $f(x) \leqslant_B f(y)$, giving $x \leqslant_A y$. □

Theorem 3.51. *If $\langle A, \leqslant_A \rangle$ and $\langle B, \leqslant_B \rangle$ are partially ordered classes and $f: A \rightarrow B$ a order isomorphism then*

$$x <_A y \Leftrightarrow f(x) <_B f(y)$$

Proof.

⇒. If $x <_A y$ then $x \neq y$ and $x \leqslant_A y \Rightarrow f(x) \leqslant_B f(y)$. Assume that $f(x) = f(y)$ then as f is a bijection we would have $x = y$ contradicting $x \neq y$. So we must have that $f(x) \neq f(y)$ hence

$$f(x) <_B f(y)$$

$\Leftarrow$. As $f(x) <_B f(y)$ we have that $f(x) \neq f(y)$ so that we must have $x \neq y$. Further as f is a isomorphism we have $x \leqslant_A y$. So

$$x <_A y$$

□

Theorem 3.52. *If $\langle A, \leqslant_A \rangle$ and $\langle B, \leqslant_B \rangle$ are partially ordered classes and $f: A \rightarrow B$ a bijection then*

$$f: A \rightarrow B \text{ is a order isomorphism} \Leftrightarrow f: A \rightarrow B \text{ and } f^{-1}: B \rightarrow A \text{ are increasing functions}$$

Proof. As $f: A \rightarrow B$ is a bijection we have by [theorems: 2.63, 2.67] that $f^{=1}: B \rightarrow A$ is a bijection.

$\Rightarrow$. As $f: A \rightarrow B$ is a isomorphism we have that $\forall x, y \in A$ with $x \leqslant_A y \Rightarrow f(x) \leqslant f(b)$ hence $f: A \rightarrow B$ is increasing. If $x, y \in B$ with $x \leqslant_B y$ then

$$f(f^{-1}(x)) = (f \circ f^{-1})(x) \underset{[\text{theorem: } 2.64}{=} x \leqslant_B y = (f \circ f^{-1})(y) = f(f^{-1}(y))$$

which as f is a isomorphism proves that $f^{-1}(x) \leqslant_A f^{-1}(y)$, hence f^{-1} is increasing.

$\Leftarrow$. Suppose that f, f^{-1} are increasing functions then if $x \leqslant_A y \underset{f \text{ is increasing}}{\Rightarrow} f(x) \leqslant_B f(y)$. Further if $f(x) \leqslant_B f(y) \underset{f^{-1} \text{ is increasing}}{\Rightarrow} f^{-1}(f(x)) \leqslant_A f^{-1}(f(y)) \Rightarrow x \leqslant y$ □

Theorem 3.53. *If $\langle A, \leqslant_A \rangle$ and $\langle B, \leqslant_B \rangle$ are partially ordered classes then*

1. *$1_A: A \rightarrow A$ is a order isomorphism*
2. *If $f: A \rightarrow B$ is a order isomorphism then $f^{-1}: B \rightarrow A$ is a order isomorphism*
3. *If $f: A \rightarrow B$ and $g: B \rightarrow C$ are order isomorphism's then $g \circ f$ is a order isomorphism*

Proof.

1. By 2.42 we have that $\mathrm{Id}_A: A \rightarrow A$ is a bijection then, as $x = I_A(x)$ and $y = \mathrm{Id}_A(y)$, we have $x \leqslant y \Leftrightarrow \mathrm{Id}_A(x) \leqslant \mathrm{Id}_A(y)$.
2. If $f: A \rightarrow B$ is a isomorphism then by [theorem: 2.67] we have that $f^{-1}: B \rightarrow A$ is a bijection. By the previous theorem [theorem: 3.52] we have that f^{-1} is increasing. Further as by 2.68 $f = (f^{-1})^{-1}$ and by [theorem: 3.52] f is increasing it follows that $(f^{-1})^{-1}$ is increasing. Using then [theorem: 3.52] it follows that f^{-1} is a isomorphism.
3. This follows from [theorem: 3.50] □

Theorem 3.54. *If $\langle A, \leqslant_A \rangle$, $\langle B, \leqslant_B \rangle$ and $\langle C, \leqslant_C \rangle$ are partially ordered classes then we have*

1. *$A \cong A$*
2. *If $A \cong B$ then $B \cong A$*
3. *If $A \cong B$ and $B \cong D$ then $B \cong D$*

Proof. This follows easily from the previous theorem [theorem: 3.53] □

Theorem 3.55. *Let $\langle A, \leqslant_A \rangle$. be a totally ordered class and $\langle B, \leqslant_B \rangle$ is a partially ordered class then a bijective and increasing function $f: A \rightarrow B$ is a isomorphism*

Proof. Suppose that $f(x) \leqslant_B f(y)$ then since A is fully ordered we have that x, y are comparable therefore by [theorem: 3.36] we have the following exclusive cases

1. $x \leqslant_A y$ in this case our theorem is proved
2. $y <_A x$ in this case we would have $f(y) \leqslant_B f(x) \Rightarrow f(y) = f(x) \underset{f \text{ is injective}}{\Rightarrow} x = y$ a contradiction. So this case does not occurs. □

3.3.3 Min, max, supremum and infinum

Definition 3.56. *Let* $\langle X, \leqslant \rangle$ *be a pre-ordered class and* $A \subseteq X$ *then*

1. m *is a* ***maximal element*** *of* A *iff* $m \in A$ *and if* $\forall x \in A$ *with* $m \leqslant x$ *we have* $x = m$
2. m *is a* ***minimal element*** *of* A *iff* $m \in A$ *and if* $\forall x \in A$ *with* $x \leqslant m$ *we have* $x = m$

Definition 3.57. *If* $\langle X, \leqslant \rangle$ *is a partial ordered class and* $A \subseteq X$ *then*

1. m *is the* ***greatest element*** *of* A *iff* $m \in A$ *and* $\forall x \in A$ *we have* $x \leqslant m$
2. m *is the* ***least element*** *of* A *iff* $m \in A$ *and* $\forall x \in A$ *we have* $m \leqslant x$

Note 3.58. There is a subtle difference between the definition of a maximal (minimal) element and the greatest (least) element. If m is the greatest (least) element of A then every element in A is comparable with m, which is not the case if m is a maximal (minimal) element of A.

Note 3.59. The empty set $\varnothing$ can not have a maximal, minimal element, greatest element or least element.

Theorem 3.60. *If* $\langle X, \leqslant \rangle$ *is a partial ordered class and* $A \subseteq X$ *then*

1. *If* m, m' *are greatest elements of* A *then* $m = m'$
2. *If* m, m' *are least elements of* A *then* $m = m'$

The unique greatest element of A *(if it exist) is called the maximum of* A *and noted as* $\max(A)$*, the unique least element of* A *(if it exist) is called the minimum of* A *and noted as* $\min(A)$

Proof.

1. If m, m' are greatest elements of A then as $m, m' \in A$ we have $m \leqslant m' \wedge m' \leqslant m$ so that $m = m'$.
2. If m, m' are least elements of A then as $m, m' \in A$ we have $m \leqslant m' \wedge m' \leqslant m$ so that $m = m'$. □

Theorem 3.61. *If* $\langle X, \leqslant \rangle$ *is a partial ordered class and* $A \subseteq X$ *such that* $\min(A)$ *and* $\max(A)$ *exist then* $\min(A) \leqslant \max(A)$

Proof. As $\min(A) \in A$ we have by definition that $\min(A) \leqslant \max(A)$. □

Theorem 3.62. *Let* $\langle X, \leqslant \rangle$ *be a partial ordered class,* $A \subseteq X$*,* $B \subseteq X$ *then*

1. *If* $\max(A)$ *and* $\max(B)$ *exist and* $\forall x \in A$ $\exists y \in B$ *such that* $x \leqslant y$ *then* $\max(A) \leqslant \max(B)$
2. *If* $\min(A)$ *and* $\min(B)$ *exist* $\forall x \in B$ $\exists y \in A$ *such that* $y \leqslant x$ *then then* $\min(A) \leqslant \min(B)$

Proof.

1. As $\max(A) \in A$ there exist a $y \in B$ such that $\max(A) \leqslant y$, as $y \leqslant \max(B)$ we have
$$\max(A) \leqslant \max(B)$$
2. As $\min(B) \in A$ there exist a $y \in A$ such that $y \leqslant \min(B)$, as $\min(A) \leqslant y$ we have
$$\min(A) \leqslant \max(A)$$
□

Definition 3.63. *If* $\langle X, \leqslant \rangle$ *is a partial ordered class and* $A \subseteq X$ *then*

1. $u \in X$ *is a* ***upper bound*** *of* A *if* $\forall a \in A$ $a \leqslant u$*.*
2. A *is* ***bounded above*** *if it has a upper bound.*
3. $l \in X$ *is a* ***lower bound*** *of* A *if* $\forall x \in A$ $l \leqslant a$
4. A *is* ***bounded below*** *if it has a lower bound.*

5. $\upsilon(A)=\{x\in X|x$ *is a upper bound of* $A\}$ *[the class of upper bound of A]*
6. $\lambda(A)=\{x\in X|x$ *is a lower bound of* $A\}$ *[the class of lower bounds of A]*

Example 3.64. If $\langle X,\leqslant\rangle$ then $\upsilon(\varnothing)=X$ and $\lambda(\varnothing)=X$

Proof. Let $x\in X$ then as $\forall a\in\varnothing\ a\leqslant x$ [or $x\leqslant a$] is vacuously satisfied $X\subseteq\upsilon(A)$ and $X\subseteq\lambda(A)$, which as $\upsilon(X)\subseteq X$ and $\lambda(X)\subseteq X$ proves $\upsilon(A)=X=\lambda(A)$. □

Definition 3.65. *If* $\langle X,\leqslant\rangle$ *is a partial ordered class and* $A\subseteq X$ *then*

1. *If* $\min(\upsilon(A))$ *exists then* $\min(\upsilon(A))$ *is called the supremum of* A *and noted as* $\sup(A)$.
2. *If* $\max(\lambda(A))$ *exists then* $\max(\lambda(A))$ *is called the infinum of* A *and noted as* $\inf(A)$

In other words if $\upsilon(A)$ has a least element then the supremum of A is this unique, by [theorem: 3.60], element. So $\sup(A)$ is the least upper bound of A [if it exist] and it is itself a upper bound. If $\lambda(A)$ has a least element then the infinum of A is this unique, by [theorem: 3.60], element. So $\inf(A)$ is the greatest lower bound [if it exist] and it is itself a lower bound.

Example 3.66. Let $\mathcal{A}$ be a class of classes and $\langle\mathcal{A},\leqslant\rangle$ the partial class where

$$\leqslant=\{(x,y)\in\mathcal{A}\times\mathcal{A}|x\subseteq y\}$$

[see example: 3.32] and $\mathcal{B}\subseteq\mathcal{A}$ we have that

1. If $\bigcap\mathcal{B}\in\mathcal{A}$ then $\inf(\mathcal{B})$ exist and $\inf(\mathcal{B})=\bigcap\mathcal{B}$
2. If $\bigcup\mathcal{B}\in\mathcal{A}$ then $\sup(\mathcal{B})$ exist and $\sup(\mathcal{B})=\bigcup\mathcal{B}$

Proof.

1. If $B\in\mathcal{B}$ then by [theorem: 1.60] $\bigcap\mathcal{B}\subseteq B\Rightarrow\bigcap\mathcal{B}\leqslant B$ so that $\bigcap\mathcal{B}\in\lambda(\mathcal{B})$. Now if $C\in\lambda(\mathcal{B})$ then $\forall B\in\mathcal{B}$ we have that $C\leqslant B\Rightarrow C\subseteq B$, so that by [theorem: 1.60] we have $C\subseteq\bigcap\mathcal{B}\Rightarrow C\leqslant\bigcap\mathcal{B}$ so that $\bigcap\mathcal{B}$ is the greatest element of $\lambda(\mathcal{B})$ proving that $\inf(\mathcal{B})$ exists and $\inf(\mathcal{B})=\bigcap\mathcal{B}$.
2. If $B\in\mathcal{B}$ then by [theorem: 1.60] $B\subseteq\bigcup\mathcal{B}\Rightarrow B\leqslant\bigcup\mathcal{B}$ so that $\bigcup\mathcal{B}\in\upsilon(\mathcal{B})$. Now if $C\in\upsilon(\mathcal{B})$ then $\forall B\in\mathcal{B}$ we have that $B\leqslant C\Rightarrow B\subseteq C$, so that by [theorem: 1.60] we have $\bigcup\mathcal{B}\subseteq C\Rightarrow\bigcup\mathcal{B}\leqslant C$ so that $\bigcup\mathcal{B}$ is the lowest element of $\upsilon(\mathcal{B})$ proving that $\sup(\mathcal{B})$ exists and $\sup(\mathcal{B})=\bigcup\mathcal{B}$. □

The following theorem will be used a lot of time when dealing with supremums and infinums.

Theorem 3.67. *Let* $\langle X,\leqslant\rangle$ *be a totally ordered set and* $A\subseteq X$ *then*

1. *If* $\sup(A)$ *exists then* $\forall x\in X$ *with* $x<\sup(A)$ *there* $\exists a\in A$ *such that* $x<a\wedge a\leqslant\sup(A)$
2. *If* $\inf(A)$ *exist then* $\forall x\in X$ *with* $\inf(A)<x$ *there* $\exists a\in A$ *such that* $\inf(A)\leqslant a\wedge a<x$

Proof. First as $\langle X,\leqslant\rangle$ is totally ordered we have $\forall x,y\in X$ that x,y are comparable, hence by [theorem: 3.37], we have $x\leqslant y\wedge y<x/$

1. Let $x\in X$ such that $x<\sup(A)$. Assume that $\forall a\in A$ we have $\neg(x<a)$ so that $a\leqslant x$, so x is a upper bound of A, hence $x\in\upsilon(A)$, so that $\sup(A)=\min(\upsilon(A))\leqslant x$, which, as $x<\sup(A)$, leads to the contradiction $x<x$. So we must have that $\exists a\in A$ such that $x<a$, further as $\sup(A)$ is a upper bound we have that $a\leqslant\sup(A)$. So
$$\exists a\in A\ \ x<a\wedge a\leqslant\sup(A)$$
2. Let $x\in X$ such that $\inf(A)<x$. Assume that $\forall a\in A$ we have $\neg(a<x)$ so that $x\leqslant a$, so x is a lower bound of A, hence $x\in\lambda(A)$, so that $x\leqslant\max(\lambda(A))=\inf(A)$, which, as $\inf(A)<x$, leads to the contradiction $x<x$. So we must have that $\exists a\in A$ such that $a\leqslant x$, further as $\inf(A)$ is a lower bound we have we have that $\inf(A)\leqslant a$. So
$$\exists a\in A\ \inf(A)\leqslant a\wedge a<x$$
□

Lemma 3.68. *If $\langle X, \leqslant \rangle$ is a partially ordered class and $A \subseteq X, B \subseteq X$ with $A \subseteq B$ then*

1. *If* $\max(A)$ *and* $\max(B)$ *exist then* $\max(A) \leqslant \max(B)$
2. *If* $\min(A)$ *and* $\min(B)$ *exists then* $\min(B) \leqslant \min(A)$

Proof.

1. As $\max(A) \in A$ and $A \subseteq B$ we have that $\max(A) \in B$ so that $\max(A) \leqslant \max(B)$
2. As $\min(A) \in A$ and $A \subseteq B$ we have that $\min(A) \in B$ so that $\min(B) \leqslant \min(A)$ □

Lemma 3.69. *If $\langle X, \leqslant \rangle$ is a partially ordered class and $A \subseteq X, B \subseteq X$ with $A \subseteq B$ then*

1. $\upsilon(B) \subseteq \upsilon(A)$
2. $\lambda(B) \subseteq \lambda(A)$

Proof.

1. Let $x \in \upsilon(B)$ then $\forall a \in A$ we have, as $A \subseteq B$ that $a \in B$ hence $a \leqslant x$ proving that x is a upper bound of A or $x \in \upsilon(A)$.
2. Let $x \in \lambda(B)$ then $\forall a \in A$ we have as $A \subseteq B$ hat $a \in B$ hence $x \leqslant a$ proving that x is a lower bound of A or $x \in \lambda(A)$. □

Theorem 3.70. *Let $\langle X, \leqslant \rangle$ be a partial ordered class and $A \subseteq X$, $B \subseteq Y$ such that $A \subseteq B$ then*

1. *If* $\sup(A)$ *and* $\sup(B)$ *exist then* $\sup(A) \leqslant \sup(B)$
2. *If* $\inf(A)$ *and* $\inf(B)$ *exist then* $\inf(B) \leqslant \inf(A)$

Proof.

1. Using [lemma: 3.69] we have that $\upsilon(B) \subseteq \upsilon(A)$ so that by [lemma: 3.68]
$$\sup(A) = \min(\upsilon(A)) \leqslant \min(\upsilon(B)) = \sup(B)$$
2. Using [lemma: 3.69] we have that $\lambda(B) \subseteq \lambda(A)$ so that by [lemma: 3.68]
$$\inf(B) = \max(\lambda(B)) \leqslant \max(\lambda(A)) = \inf(A)$$
□

Theorem 3.71. *Let $\langle X, \leqslant \rangle$ be a partial ordered class and $A \subseteq X, B \subseteq X$ then*

1. *If* $\sup(A)$, $\sup(B)$ *exists and* $\forall a \in A$ $\exists b \in B$ *such that* $a \leqslant b$ *then* $\sup(A) \leqslant \sup(B)$
2. *If* $\inf(A)$ *and* $\inf(B)$ *exist and* $\forall a \in A$ $\exists b \in B$ *such that* $b \leqslant a$ *then* $\inf(B) \leqslant \inf(A)$

Proof.

1. Let $a \in A$ then $\exists b \in B$ such that $a \leqslant b$, as $b \leqslant \sup(B)$ it follows that $a \leqslant \sup(B)$. Hence $\sup(B) \in \upsilon(A)$. So $\sup(A) = \min(\upsilon(A)) \leqslant \sup(A)$, hence
$$\sup(A) \leqslant \sup(B)$$
2. Let $a \in A$ then $\exists b \in B$ such that $b \leqslant a$, as $\inf(B) \leqslant b$ it follows that $\inf(B) \leqslant a$. Hence $\inf(B) \in \lambda(A)$, So $\inf(B) \leqslant \max(\lambda(A)) = \inf(A)$, hence
$$\inf(B) \leqslant \inf(A)$$
□

We have by definition that $\sup(A)$ exists if $\min(\upsilon(A))$ exists and $\inf(A)$ exist if $\max(\lambda(A))$ exist. The following theorem shows that there is a weaker condition for the existence of $\sup(A)$ and $\inf(A)$.

Theorem 3.72. *Let $\langle X, \leqslant \rangle$ be a partial ordered class and $A \subseteq X$ then*

1. *If $\lambda(A)$ has a supremum then A has a infinum and* $\sup(\lambda(A)) = \inf(A)$

2. *If $\upsilon(A)$ has a infinum then A has a supremum and* $\inf(\upsilon(A)) = \sup(A)$

Proof.

1. If $a \in A$ then $\forall y \in \lambda(A)$ we have $y \leqslant a$ so that $a \in \upsilon(\lambda(A))$. As $\sup(\lambda(A)) = \min(\upsilon(\lambda(A)))$ we have that $\sup(\lambda(A)) \leqslant a$. As $a \in A$ was arbitrary chosen we have that

$$\sup(\lambda(A)) \in \lambda(A) \tag{3.8}$$

If $x \in \lambda(A)$, then, as $\sup(\lambda(A))$ is a upper bound of $\lambda(A)$, we have $x \leqslant \sup(\lambda(A))$. So

$$\forall x \in \lambda(A) \text{ we have } x \leqslant \sup(\lambda(A)) \tag{3.9}$$

Using [eq: 3.8] and [eq: 3.9] it follows that $\sup(\lambda(A)) = \max(\lambda(A)) = \inf(A)$ or

$$\sup(\lambda(A)) = \inf(A)$$

2. If $a \in A$ then $\forall y \in \upsilon(A)$ we have $a \leqslant y$ so that $a \in \lambda(\upsilon(A))$. As $\inf(\upsilon(A)) = \max(\lambda(\upsilon(A)))$ we have that $a \leqslant \inf(\upsilon(A))$. As $a \in A$ was arbitrary chosen we have that

$$\inf(\upsilon(A)) \in \upsilon(A) \tag{3.10}$$

If $x \in \upsilon(A)$, then, as $\inf(\upsilon(A))$ is a lower bound of $\upsilon(A)$, we have $\inf(\upsilon(A)) \leqslant x$. So we have that

$$\forall x \in \upsilon(A) \text{ we have that } \inf(\upsilon(A)) \leqslant x \tag{3.11}$$

Using [eq: 3.10] and [eq: 3.11] it follows that $\inf(\upsilon(A)) = \min(\upsilon(A)) = \sup(A)$ or

$$\inf(\upsilon(A)) = \sup(A)$$

□

In general it is not guaranteed that $\sup(A)$ or $\inf(A)$ exists. However there exists partial order classes that guarantees the existence of a supremum for non empty sub-classes that are bounded above.

Definition 3.73. (Conditional Completeness) *A partial ordered class $\langle X, \leqslant\rangle$ is **conditional complete** if every non empty sub-class of A that is bounded above has a supremum.*

The next theorem shows that conditional completeness can also be defined based on bounded below and infinum.

Theorem 3.74. *If $\langle A, \leqslant\rangle$ is a partial ordered class then the following are equivalent*

1. *Every non empty sub-class of X that is bounded above has a supremum [$\langle X, \leqslant\rangle$ is conditional complete]*
2. *Every non empty sub-class of X that is bounded below has a infinum*

Proof.

1 ⇒ 2. Let $A \subseteq X$ a non empty sub-class that is bounded below. As $A \neq \varnothing$ there exists a $a \in A$, further by definition of $\lambda(A)$ we have $\forall y \in \lambda(A)$ that $y \leqslant a$ so $\lambda(A)$ is bounded above. As A is bounded below we have that $\lambda(A) \neq \varnothing$. So by the hypothesis $\sup(\lambda(A))$ exist. Applying then [theorem: 3.72] proves

$$\inf(A) \text{ exist}$$

2 ⇒ 1. Let $A \subseteq X$ a non empty sub-class that is bounded above. As $A \neq \varnothing$ there exists a $a \in A$, further by definition of $\upsilon(A)$ we have $\forall y \in \upsilon(A)$ that $a \leqslant y$ so $\upsilon(A)$ is bounded below. As A is bounded above we have that $\upsilon(A) \neq \varnothing$. So by the hypothesis $\inf(\upsilon(A))$ exist. Applying then [theorem: 3.72] proves

$$\sup(A) \text{ exist}$$

□

Next we show that a order isomorphism preserves the concepts of greatest element, least element, upper bound, lower bound, supremum and infinum.

Lemma 3.75. *Let $\langle X, \leqslant_X \rangle$, $\langle Y, \leqslant_Y \rangle$ be partial ordered classes, $f: X \rightarrow Y$ is a order isomorphism, $A \subseteq X$ and $B \subseteq Y$ then*

1. *If u is a upper bound of B then $(f^{-1})(u)$ is a upper bound of $f^{-1}(B)$*
2. *If l is a lower bound of B then $(f^{-1})(l)$ is a lower bound of $f^{-1}(B)$*
3. *If u is a upper bound of A then $f(u)$ is a upper bound of $f(A)$*
4. *If l is a lower bound of A then $f(u)$ is a lower bound of $f(A)$*
5. $f(\upsilon(A)) = \upsilon(f(A))$
6. $f(\lambda(A)) = \lambda(f(A))$
7. *If* $\max(A)$ *exist then* $\max(f(A))$ *exist and* $\max(f(A)) = f(\max(A))$
8. *If* $\min(A)$ *exist then* $\min(f(A))$ *exist and* $\min(f(A)) = f(\min(A))$
9. *If* $\sup(A)$ *exist then* $\sup(f(A))$ *exist and* $\sup(f(A)) = f(\sup(A))$
10. *If* $\inf(A)$ *exist then* $\inf(f(A))$ *exist and* $\inf(f(A)) = f(\inf(A))$

Proof. First using [theorem: 3.52] we have that $f: X \rightarrow Y$ and $f^{-1}: Y \rightarrow X$ are increasing.

1. Let $x \in f^{-1}(B)$ then $\exists y \in B$ such that $y = f(x)$, as u is a upper bound of B, we have that $y \leqslant_B u$. So $x \underset{\text{[theorem: 2.65]}}{=} (f^{-1})(f(x)) = (f^{-1})(y) \leqslant_A (f^{-1})(u)$, proving that $(f^{-1})(u)$ is a upper bound of $f^{-1}(B)$.
2. Let $x \in f^{-1}(B)$ then $\exists y \in B$ such that $y = f(x)$, as l is a lower bound of B we have that $l \leqslant_B y$. So $(f^{-1})(l) \leqslant_A (f^{-1})(y) = (f^{-1})(f(x)) \underset{\text{[theorem: 2.65]}}{=} x$, proving that $(f^{-1})(l)$ is a lower bound of $f^{-1}(B)$.
3. If $y \in f(A)$ then $\exists x \in A$ such that $y = f(x)$. As u is a upper bound of A we have that $x \leqslant_A u$, so $y = f(x) \leqslant_B f(u)$ proving that $f(u)$ is a upper bound of $f(A)$.
4. If $y \in f(A)$ then $\exists x \in A$ such that $y = f(x)$, As l is a lower bound of A we have that $l \leqslant_A x$, so $f(l) \leqslant_B f(x) = y$ proving that $f(l)$ is a lower bound of $f(A)$.
5. If $y \in f(\upsilon(A))$ then there $\exists x \in \upsilon(A)$ such that $y = f(x)$. As $x \in \upsilon(A)$, x is a upper bound of B, so that by (3) $y = f(x)$ is a upper bound of $f(A)$. Hence

   $$f(\upsilon(A)) \subseteq \upsilon(f(A)) \tag{3.12}$$

   If $y \in \upsilon(f(A))$ then by (1) $(f^{-1})(y)$ is a upper bound of $f^{-1}(f(A)) \underset{\text{[theorem: 2.51]}}{=} A$ so that $(f^{-1})(y) \in \upsilon(A)$. So $y \underset{\text{[theorem: 2.65}}{=} f((f^{-1})(y)) = y \in f(\upsilon(A))$. Hence $\upsilon(f(A)) \subseteq f(\upsilon(A))$ which combined with [eq: 3.12] proves

   $$f(\upsilon(A)) = \upsilon(f(A))$$

6. If $y \in f(\lambda(A))$ then there $\exists x \in \lambda(A)$ such that $y = f(x)$. As $x \in \lambda(A)$, x is a lower bound of A, so that by (4) $y = f(x)$ is a lower bound of $f(A)$. Hence

   $$f(\lambda(A)) \subseteq \lambda(f(A)) \tag{3.13}$$

   If $y \in \lambda(f(A))$ then by (2) $(f^{-1})(y)$ is a lower bound of $f^{-1}(f(A)) \underset{\text{[theorem: 2.51]}}{=} A$ so that $(f^{-1})(y) \in \lambda(A)$. So $y \underset{\text{[theorem: 2.65}}{=} f((f^{-1})(y)) = y \in f(\lambda(A))$. Hence $\lambda(f(A)) \subseteq f(\lambda(A))$ which combined with [eq: 3.12] proves

   $$f(\lambda(A)) = \lambda(f(A))$$

7. If $\max(A)$ exist then $\max(A) \in A$ giving $f(\max(A)) \in f(A)$. Let $y \in f(A)$ then $\exists x \in A$ such that $y = f(x)$, as $\max(A)$ exist we have $x \leqslant_A \max(A)$ so that $y = f(x) \leqslant_B f(\max(A))$. So

$$\max(f(A)) \text{ exist and } \max(f(A)) = f(\max(A))$$

8. If $\min(A)$ exist then $\min(A) \in A$ giving $f(\min(A)) \in f(A)$. Let $y \in f(A)$ then $\exists x \in A$ such that $y = f(x)$, as $\min(A)$ exist we have $\min(A) \leqslant_A x$ so that $f(\min(A)) \leqslant_B f(x) = y$. So

$$\min(f(A)) \text{ exist and } \min(f(A)) = f(\min(A))$$

9. If $\sup(A)$ exists then $\min(\upsilon(A))$ exists and $\sup(A) = \min(\upsilon(A))$. Using (8) $\min(f(\upsilon(A)))$ exist, As $f(\upsilon(A)) \underset{(5)}{=} \upsilon(f(A))$ we have that $\min(\upsilon(f(A)))$ exist and

$$\sup(f(A)) = \min(\upsilon(f(A))) \underset{(5)}{=} \min(f(\upsilon(A))) \underset{(8)}{=} f(\min(\upsilon(A))) = f(\sup(A))$$

10. If $\inf(A)$ exists then $\max(\lambda(A))$ exists and $\inf(A) = \max(\lambda(A))$. Using (7) $\max(f(\lambda(A)))$ exist, As $f(\lambda(A)) \underset{(6)}{=} \lambda(f(A))$ we have that $\max(\lambda(f(A)))$ exist and

$$\inf(f(A)) = \max(\lambda(f(A))) \underset{(6)}{=} \max(f(\lambda(A))) \underset{(7)}{=} f(\max(\lambda(A))) = f(\inf(A))$$ □

Theorem 3.76. *Let $\langle X, \leqslant_X \rangle$ be a conditional complete partial ordered set, $\langle Y, \leqslant_Y \rangle$ a partial ordered class and $f: X \rightarrow Y$ a order isomorphism then $\langle Y, \leqslant_Y \rangle$ is conditionally complete.*

Proof. Let $A \subseteq Y$ be such that A is bounded above and non empty. Let u be a upper bound of A then by [lemma: 3.75] we have that $(f^{-1})(u)$ is a upper bound of $f^{-1}(A)$. As $A \neq \varnothing$ there exists a $a \in A$ which as f is surjective means that $\exists x$ such that $a = f(x)$ hence $x \in f^{-1}(A)$ proving that $f^{-1}(A) \neq \varnothing$. As $\langle X, \leqslant_X \rangle$ is conditional complete $\sup(f^{-1}(A))$ exist. Using [lemma: 3.75] $\sup(f(f^{-1}(A)))$ exist which as $A \underset{\text{[theorem: 2.51]}}{=} f(f^{-1}(A))$ proves that $\sup(A)$ exist. So $\langle X, \leqslant_Y \rangle$ is conditional complete. □

3.3.4 Well ordering

Definition 3.77. *A partial ordered class $\langle X, \leqslant \rangle$ is* ***well ordered*** *is every non empty sub-class of X has a least element. In other words if $\forall A \in \mathcal{P}(X)$ $\min(A)$ exist.*

Theorem 3.78. *If $\langle X, \leqslant \rangle$ is a partial ordered class, $B \subseteq X$ then for $\langle B, \leqslant_{|B} \rangle$ [see theorem: 3.34] we have*

1. *If $\langle X, \leqslant \rangle$ is totally ordered then $\langle B, \leqslant_{|B} \rangle$ is totally ordered*
2. *If $\langle X, \leqslant \rangle$ is well ordered then $\langle B, \leqslant_{|B} \rangle$ is totally ordered*

Proof.

1. If $x, y \in B \Rightarrow x, y \in X$ hence $x \leqslant y \vee y \leqslant x$ so that $x \leqslant_{|B} y \vee y \leqslant_{|B} x$.
2. If $C \subseteq B$ is a non empty class then as $B \subseteq X$ we have $\varnothing \neq C \subseteq X$. So there exists a least element c of C. So $c \in C$ and $\forall x \in C$ we have $c \leqslant x \underset{x \in B}{\Rightarrow} c \leqslant_{|B} x$ proving that c is a least element of C using the order relation $\leqslant_{|B}$. □

Well ordering is a stronger condition then conditional completeness and totally ordering

Theorem 3.79. *Let $\langle X, \leqslant \rangle$ is a well ordered class then*

1. *$\langle X, \leqslant \rangle$ is totally ordered*
2. *$\langle X, \leqslant \rangle$ is conditional complete*
3. *$\forall x, y \in X$ we have $x \leqslant y$ or $y < x$*

Proof.

1. If $x, y \in X$ then $\{x, y\}$ is a non empty sub-class of X and must have a least element. If x is the least element then $x \leqslant y$ and if y is the least element then $y \leqslant x$, so $\langle X, \leqslant \rangle$ is totally ordered.

2. If A is a non empty sub-class of X that is bounded above then $\upsilon(A) \neq \varnothing$. Using well ordering we have that $\sup(A) = \min(\upsilon(A))$ exist.

3. As by (1) $\langle X, \leqslant \rangle$ is totally ordered we have that x and y are comparable, hence by [theorem: 3.37] we have $x \leqslant y \vee y < x$. □

One difference between the order relation on the set of whole numbers $\mathbb{Z}$ and the set of real numbers $\mathbb{R}$ is that there does not exist a whole number between 1 and 2 while for the real numbers there is the real number 1.5 between 1 and 2. This leads to the following definition.

Definition 3.80. (Immediate successor) *Let $\langle X, \leqslant \rangle$ be a partial ordered set and $x, y \in X$ then y is the **immediate** successor of x iff*

1. *$x < y$*
2. *$\neg(\exists z \in X$ such that $x < z \wedge z < y)$ [in words there does not exists a $x \in X$ such that $x < z < y$]*

Theorem 3.81. *Let $\langle X, \leqslant \rangle$ be a well ordered class then every element that is not a greatest element of X has a immediate successor.*

Proof. Using [theorem: 3.79] we have that $\langle X, \leqslant \rangle$ is totally ordered. Let $x \in X$ such that x is not a greatest element in X. Take $B = \{y \in X | x < y\}$ then if $B = \varnothing$ we have that $X \setminus B = X$ so $\forall r \in X$ we have $r \notin B$ or $\neg(x < r)$, by [theorem: 3.79] we have that $r \leqslant x$, proving that x is a greatest element of X which contradicts or hypothesis.. So we must have that $B \neq \varnothing$, by well ordering there exist a least element b of B, which as $b \in B$ gives $x < b$. Assume that there exist a $a \in X$ such that $x < a \wedge a < b$, then we must have that $a \in B$ and $a < b$. As b is the least element of B and $a \in B$ we have $b < a$ leading to the contradiction $a < a$. So b is a immediate successor of $x/$ □

Definition 3.82. *Let $\langle X, \leqslant \rangle$ be a partial ordered class then $B \subseteq A$ is a **section** of X if*

$$\forall x \in X \text{ we have } \forall y \in B \textit{ with } x \leqslant y \textit{ that } x \in B$$

Lemma 3.83. *Let $\langle X, \leqslant \rangle$ be a well ordered class and $B \subseteq X$ then*

B is a section $\Leftrightarrow$ $B = X$ or B is a initial segment of X [definition: 3.44]

Proof.

⇒. Let B be a section of X then if $B = X$ we are done. So we must prove the theorem for $B \neq X$ or equivalently $X \setminus B \neq \varnothing$. Because X is well ordered, there a exists a least element $l \in X \setminus B$. Consider the initial segment $S_{X,l} = \{x \in X | x < l\}$ [see definition: 3.44]. Let $x \in S_{X,l}$ so that $x < l$. Assume that $x \notin B$ then $x \in X \setminus B$ so, as l is a least element of $X \setminus B$, we have $l \leqslant x$ which combined with $x < l$ leads to the contradiction $l < l$. So we must have that $x \in B$ which proves that

$$S_{X,l} \subseteq B \tag{3.14}$$

Let $x \in B$, as X is well ordered we have by [theorem: 3.79] that $l \leqslant x \vee x < l$. Assume that $l \leqslant x$ then, as B is a section, we have $l \in B$ contradicting $l \in X \setminus B$ [as l is least element of $X \setminus B$]. So we must have $x < l$ or $x \in S_{X,l}$ so $B \subseteq S_{X,l}$. Combining this result with [eq: 3.14] proves

$$S_{X,l} = B$$

⇐. If $X = B$ then $\forall x \in X$ we have $\forall y \in B = X$ with $x \leqslant y$ that trivially $x \in X = B$, so B is a section. If B is initial segment then there exist a $l \in X$ such that $B = \{y \in X | y < l\}$. Take $x \in X$ then if $y \in B$ with $x \leqslant y$ we have $y < l$ so that $x < l$ hence $x \in B$, proving that B is a section. □

A application of the above lemma is Transfinite Induction.

Theorem 3.84. **(Transfinite Induction)** *Let $\langle X, \leqslant\rangle$ be a well ordered class and let $P(x)$ a proposition about x [a statement about x that can be true or false] such that*

$$\forall x \in X \text{ such that, if } P(y) \text{ is true for every } y < x \text{ then } P(x) \text{ is true} \tag{3.15}$$

then

$$\forall x \in X\ P(x) \text{ is true}$$

Proof. We prove this by contradiction. Assume that $\exists x \in X$ such that $P(x)$ is false, then $B = \{x \in X | \mathcal{P}(x) \text{ is false}\}$ is non empty. As X is well ordered there exist a least element $l \in B$. Take $x \in X$ with $x < l$ then $x \notin B$ [for if $x \in B$ then $l \leqslant x$, which combined with $x < l$ gives the contradiction $l < l$] so that $P(x)$ is true. By the hypothesis [eq: 3.15] we have that $P(l)$ is true, which means that $l \notin B$ contradicting $l \in B$. So we must have that $\forall x \in X\ P(x)$ is true. □

Lemma 3.85. *Let $\langle X, \leqslant\rangle$ be a well ordered class, $B \subseteq X$ and $f: X \rightarrow B$ a order isomorphism then $\forall x \in X$ we have $x \leqslant f(x)$*

Proof. We prove this by contradiction. Assume that that$\exists x \in X$ such that $\neg(x \leqslant f(x))$. As $\langle X, \leqslant\rangle$ if well ordered we have by [theorem: 3.79] that $f(x) < x$, hence $C = \{x \in X | f(x) < x\} \neq \varnothing$. By well ordering there exists a least element c of C. As $c \in C$ we have that $f(c) < c$, hence by [theorem: 3.51] $f(f(c)) < f(c)$ so that $f(c) \in C$. As c is the least element of C we have $c \leqslant f(c)$, which combined with $f(c) < c$ gives the contradiction $c < c$. So we must have $\forall x \in X$ that $x \leqslant f(x)$. □

Theorem 3.86. *Let $\langle X, \leqslant\rangle$ be a well ordered class then there does not exist a order isomorphism from X to a sub-class of an initial segment of X.*

Proof. We prove this by contradiction. So assume that there exists a initial segment $S_{X,a} = \{y \in X | y < a\}$ of X, a $B \subseteq S_{X,\alpha}$ and a isomorphism $f: X \rightarrow B$. Using the previous lemma [lemma: 3.85] we have that $a \leqslant f(a)$, so $f(a) \notin S_{X,a}$ [for if $f(a) \in S_{X,a}$ then $f(a) < a$ leading to the contradiction $a < a$]. However as $\text{range}(f) = B \subseteq S_{X,a}$ we must have that $f(a) \in S_{X,a}$ and we reach a contradiction. □

Corollary 3.87. *Let $\langle X, \leqslant\rangle$ be a well ordered class then there does not exist a order isomorphism between X and initial segment of X*

Proof. As a initial segment is a sub-class of itself this follows from the previous theorem [theorem: 3.86] □

Theorem 3.88. *If $\langle X, \leqslant_X\rangle$, $\langle Y, \leqslant_Y\rangle$ are well ordered classes then if X is order isomorphic with an initial segment of Y we have that Y is not order isomorphic with any sub-class of X.*

Proof. Let $S_{X,y}$ be a initial segment of Y and $f: X \rightarrow S_{X,y}$ a order isomorphism. Assume that there exist a $A \subseteq X$ and a order isomorphism $g: Y \rightarrow A$, As by [lemma: 2.28],[theorem: 2.48] and the fact that 'increasing' is a property of the graph of a function,we have that $g: Y \rightarrow X$ is a injective increasing function. Using [theorem: 2.69],[theorem: 3.50] we have that $f \circ g: Y \rightarrow S_{X,y}$ is a injective increasing function, hence $f \circ f: Y \rightarrow (f \circ g)(Y)$ is a bijective function [see theorem: 2.62] which is increasing, hence by [theorem: 3.55] we have that $f \circ g: Y \rightarrow (f \circ g)(Y)$ is a order isomorphism. As $(f \circ g)(Y) \subseteq \text{range}(f)$ [see theorem: 2.19] and $\text{range}(f) \subseteq S_{X,y}$ we have a order isomorphism between Y and a sub-class of a initial segment of Y. By [theorem: 3.86] this is impossible so the assumption is false, hence Y is not order isomorphic to a an initial segment of Y. □

Corollary 3.89. *If $\langle X, \leqslant_X\rangle$, $\langle Y, \leqslant_Y\rangle$ are well ordered classes such that X is order isomorphic with Y then*

1. *X can not be order isomorphic with a initial segment of Y*
2. *Y can not be order isomorphic with a initial segment of X*

Proof. We prove this by contradiction. First by the hypothesis we have $X \cong Y$ and by [theorem: 3.54] $Y \cong X$.

1. If X is order isomorphic with a initial segment of Y then as $Y \cong X$ we have that Y is order isomorphic with a sub-class of X, which by [theorem: 3.88] is not allowed.
2. If Y is order isomorphic with a initial segment of X then as $X \cong Y$ we have that X is order isomorphic with a sub-class of Y, which by [theorem: 3.88] is not allowed. □

Lemma 3.90. *Let $\langle X, \leqslant \rangle$ be a well ordered class and $a, b \in X$ with $a < b$ then $S_{X,a}$ is a initial segment of $\mathcal{S}_{X,b}$ [using the order $\leqslant_{|S_{X,y}}$]*

Proof. First if $x \in S_{X,a}$ then $x < a \underset{\mathrm{a<b}}{\Rightarrow} x < b$ so that $x \in S_{X,b}$, hence

$$S_{X,a} \subseteq S_{X,b}$$

Now if $x \in S_{X,b}$ and $y \in S_{X,a}$ is such that $x \leqslant_{|S_{X_B}} y$ then $x \leqslant y \underset{y \in S_{X,a} \Rightarrow y < a}{\Rightarrow} x < a$ hence $x \in S_{X,a}$. So $S_{X,a}$ is a section of $S_{X,b}$, as $a \notin S_{X,a} \wedge a \in S_{X,b}$ [for $a < b$] we have $S_{X,a} \neq S_{X,b}$ so that, using [theorem: 3.83], $S_{X,a}$ is a initial segment of $S_{X,b}$. □

Theorem 3.91. *Let Let $\langle X, \leqslant_X \rangle$ and $\langle Y, \leqslant_Y \rangle$ be well ordered classes then exactly one of the following cases hold*

1. *X is order isomorphic with Y*
2. *X is order isomorphic with an initial segment of Y*
3. *Y is order isomorphic with an initial segment of X*

Proof. Define

$$C = \{x \in X \mid \exists y \in Y \text{ such that } S_{X,x} \cong S_{Y,y}\} \tag{3.16}$$

and

$$F = \{(x, y) \in C \times Y \mid S_{X,x} \cong S_{Y,y})\tag{3.17}$$

We prove now that F is the graph of a order isomorphism between C and $F(C)$. We have trivially from the definition of F that

$$F \subseteq C \times Y \tag{3.18}$$

Let $(x, y), (x, y') \in F$, then $\mathcal{S}_{X,x} \cong S_{Y,y}$ and $S_{x,x} \cong S_{Y,y'}$ so by [theorem: 3.54]

$$S_{Y,y} \cong S_{Y,y'} \tag{3.19}$$

Assume that $y \neq y'$ then, as $\langle Y, \leqslant_Y \rangle$ is well ordered we have by [theorem: 3.79] either:

$y \leqslant y'$. then $y < y'$ so that by the previous lemma [lemma: 3.90] we have that $S_{Y,y}$ is a initial segment of $S_{Y,y'}$. Using [corollary: 3.87] we have then that $S_{Y,y'}$ is not order isomorphic with $S_{Y,y}$ contradicting [eq: 3.19].

$y' < y$. then by the previous lemma [lemma: 3.90] we have that $S_{Y,y'}$ is a initial segment of $S_{Y,y}$. Using [corollary: 3.87] we have then that $S_{Y,y}$ is not order isomorphic with $S_{Y,y'}$ contradicting [eq: 3.19].

as in all cases we have a contradiction, the assumption must be wrong. Hence

$$\text{If } (x, y), (x, y') \in F \text{ then } y = y' \tag{3.20}$$

Further if $x \in C$ then by definition of C there exists a $y \in Y$ such that $S_{X,x} = S_{Y,y}$ hence $(x, y) \in F$ proving that

$$C \subseteq \mathrm{dom}(F) \tag{3.21}$$

If $(x, y), (x', y) \in F$ then $S_{X,x} \cong S_{Y,y}$ and $\mathcal{S}_{X,x'} \cong S_{Y,y}$ so by [theorem: 3.54] we have that

$$S_{X,x} \cong S_{X,x'} \tag{3.22}$$

Assume that $x \neq x'$ then, as $\langle X, \leqslant_X \rangle$ is well ordered we have by [theorem: 3.79] either:

$x \leqslant x'$. then $x < x'$ so that by the previous lemma [lemma: 3.90] we have that $S_{X,x}$ is a initial segment of $S_{X,x'}$. Using [corollary: 3.87] we have then that $S_{X,x'}$ is not order isomorphic with $S_{X,x}$ contradicting [eq: 3.22].

$x' \leqslant x$. then by the previous lemma [lemma: 3.90] we have that $S_{X,x'}$ is a initial segment of $S_{X,x}$. Using [corollary: 3.87] we have then that $S_{X,x}$ is not order isomorphic with $S_{X,x'}$ contradicting [eq: 3.22].

as in all cases we have a contradiction, the assumption must be wrong. Hence

$$\text{If } (x, y), (x', y) \in F \text{ we have } x = x' \tag{3.23}$$

Combining [eq: 3.18], [eq: 3.20], [eq: 3.21] and [eq: 3.23] it follows that $F: C \rightarrow Y$ is a injective function. Applying then [proposition: 2.62] gives if we define $D = F(C)$

$$F: C \rightarrow D \text{ is a bijection} \tag{3.24}$$

Take $x, y \in C$ such that $x \leqslant_X y$ then by definition of F we have

$$S_{X,x} \cong S_{Y,F(x)} \text{ and } S_{X,y} \cong S_{Y,F(y)} \tag{3.25}$$

Assume now that $\neg(F(x) \leqslant_Y F(y))$ then as $\langle Y, \leqslant_Y \rangle$ is well ordered we have by [theorem: 3.79] that $F(y) <_Y F(x)$. So using [theorem: 3.90] we have that $S_{Y,F(y)}$ is a initial segment of $S_{Y,F(x)}$. As $x \leqslant_X y$ it follows that $S_{X,x} \subseteq S_{X,y}$ [see proposition: 3.45]. So we have using [eq: 3.25]

a) $S_{X,y}$ is order isomorphic with $S_{Y,F(y)}$ a initial segment of $S_{Y,F(x)}$

b) $S_{F(x)}$ is order isomorphic with $S_{X,x}$ a sub-class of $S_{X,y}$

Using [theorem: 3.88] we see that (a) and (b) can not be all true, hence our assumption is false so that $F(x) \leqslant F(y)$. Hence we have that $F: C \rightarrow D$ is a increasing bijection which by [theorem: 3.55] proves that

$$F: C \rightarrow D \text{ is a order isomorphism or } C \cong D \tag{3.26}$$

Next we prove that

$$C \text{ is a section of } X \tag{3.27}$$

Proof. Let $x \in X$ and take $c \in C$ such that $x \leqslant_X c$. As $S_{X,c} \cong S_{Y,F(c)}$ there exist a order isomorphism

$$g: S_{X,c} \rightarrow S_{Y,F(c)} \tag{3.28}$$

Now as $x \leqslant_X c$ we have by [proposition: 3.45] that $S_{X,x} \subseteq S_{X,c}$. Hence by 2.82 we have that

$$g_{|S_{X,x}}: S_{X,x} \rightarrow S_{X,c} \text{ is a function} \tag{3.29}$$

Further if $y \in S_{X,x}$ we have that $y <_X x$, so as g is a order isomorphism we have $g(y) <_Y g(x)$ proving that $g_{|S_{X,x}}(y) = g(y) \in S_{Y,g(x)}$ or $\text{range}(g_{|S_{X,x}}) \subseteq S_{Y,g(x)}$. So by [theorem: 2.32] it follows that

$$g_{|S_{X,x}}: S_{X,x} \rightarrow S_{Y,g(x)} \text{ is a function} \tag{3.30}$$

As g is a isomorphism and thus injective it follows from [theorem: 2.78] that

$$g_{|S_{X,x}}: S_{X_x} \rightarrow S_{Y,g(x)} \text{ is injective} \tag{3.31}$$

Further if $y \in S_{Y,g(x)}$ then $y <_Y g(x)$, as $g(x) \in S_{Y,F(c)}$ [see eq: 3.28] we have $g(x) <_Y F(c)$ so that $y <_Y F(c)$ proving $y \in S_{Y,F(c)}$. As g is surjective there exist a $u \in S_{X,c}$ such that $y = g(u)$. Assume that $x \leqslant_X u$ then $g(x) \leqslant_Y g(u) = y$, as $y <_Y g(x)$ this gives the contradiction $g(x) < g(x)$. So we have $\neg(x \leqslant u)$ which, as $\langle X, \leqslant_X \rangle$ is well ordered, gives by [theorem: 3.79] that $u <_X x$ so that $u \in S_{X,x}$. So for $y \in S_{Y,g(x)}$ we found a $u \in S_{X,x}$ such that $g_{|S_{X,x}}(u) = g(u) = y$ proving that

$$g_{|S_{X,x}}: S_{X,x} \rightarrow S_{Y,g(x)} \text{ is surjective} \tag{3.32}$$

Further if $u, v \in S_{X,x}$ are such that $u \leqslant_X v$ so that $g_{|S_{X,x}}(u) = g(u) \leqslant_X g(v) = g_{|S_{X,x}}(v)$ proving that

$$g_{|S_{X,x}}: S_{X,x} \rightarrow S_{Y,g(x)} \text{ is increasing} \tag{3.33}$$

Combining [eq: 3.29], [eq: 3.30], [eq: 3.32], [eq: 3.33] we have that $g_{|S_{X,x}}: S_{X,x} \rightarrow S_{Y,g(x)}$ is a order isomorphism so that $S_{X,x} \cong S_{Y,g(x)}$ hence $x \in C$. Proving that C is as section of X. □

Next we prove that

$$D \text{ is a section of } Y \tag{3.34}$$

Proof. Let $y \in Y$ and take $d \in D$ such that $y \leqslant_Y d$. As $d \in D = \text{range}(F)$ there exist a $c \in C$ such that $F(c) = d$, so $S_{X,c} \cong S_{Y,d} \underset{[\text{theorem: } 3.54]}{\Rightarrow} S_{Y,d} \cong S_{X,c}$. So there exist a order isomorphism

$$f: S_{Y,d} \rightarrow S_{X,c} \tag{3.35}$$

Now from $y \leqslant_D d$ we have by [theorem: 3.45] $S_{Y,y} \subseteq S_{Y,d}$. Hence by 2.82 we have that

$$f_{|S_{Y,y}}: S_{Y,y} \rightarrow S_{X,c} \text{ is a function} \tag{3.36}$$

If $x \in S_{Y,y}$ then $x <_Y y$ so, as f is a order isomorphism, $f_{|S_{Y,y}}(x) = f(x) <_X f(y)$, we have that $f_{|S_{Y,y}}(x) \in S_{Y,f(y)}$, so $\text{range}(f_{|S_{Y,y}}) \subseteq S_{X,f(y)}$. By [theorem: 2.32] it follows that

$$f_{|S_{Y,y}}: S_{Y,y} \rightarrow S_{X,f(y)} \text{ is a function} \tag{3.37}$$

As f is a isomorphism and injective it follows from [theorem: 2.78] that

$$f_{|S_{Y,y}}: S_{Y,y} \rightarrow S_{X,f(y)} \text{ is injective} \tag{3.38}$$

If $x \in S_{X,f(y)}$ then $x <_X f(y)$, as by [eq: 3.35] $f(y) \in S_{X,c}$, we have $f(y) < c$, so that $x <_X c$ or $x \in S_{X,c}$. As f is surjective there exists a $u \in S_{Y,d}$ such that $f(u) = x$. As $u \in S_{Y,d}$ we have that $u <_Y d$. Assume now that $y \leqslant_Y u$ then, as f is a order isomorphism, $f(y) \leqslant_X f(u) = x$, which as $x <_X f(y)$ gives the contradiction $x <_X x$. So we must have that $\neg(y \leqslant_Y u)$, which, as $\langle Y, \leqslant_Y \rangle$ is well ordered, gives by [theorem: 3.79] that $u <_Y y$ or $u \in S_{Y,y}$. So for $x \in S_{X,f(y)}$ there exist a $u \in S_{Y,y}$ such that $f(u) = x$, proving that

$$f_{|S_{Y,y}}: S_{Y,y} \rightarrow S_{X,f(y)} \text{ is surjective} \tag{3.39}$$

Further if $u, v \in S_{Y,y}$ is such that $u \leqslant v$ then $f_{|S_{Y,y}}(u) = f(u) \leqslant f(v) = f_{|S_{U,y}}(v)$ proving that

$$f_{|S_{Y,y}}: S_{Y,y} \rightarrow S_{X,f(y)} \text{ is increasing} \tag{3.40}$$

Combining [eq: 3.37], [eq: 3.38], [eq: 3.39] and [eq: 3.40] we have that $f_{|S_{Y,y}}: S_{Y,y} \rightarrow S_{X,f(y)}$ is a order isomorphism, hence $S_{Y,y} \cong S_{X,f(y)}$. As $f(y) \in S_{X,c} \subseteq X$ and $y \in Y$ it follows from the definition of C that $f(y) \in C$, hence by definition of F $(f(y), y) \in F$ or $y = F(f(y)) \in F(C) = D$, giving $y \in D$. Proving that D is a section of Y. □

To summarize [eq: 3.26], [eq: 3.27] and [eq: 3.34] we have

$$C \cong D \wedge C \text{ is a segment of } X \wedge D \text{ is a segment of } Y \tag{3.41}$$

Assume now that C is a initial segment of X and D is a initial segment of Y then there exist a $r \in X$ and a $s \in Y$ such that $C = S_{X,r}$ and $D = S_{Y,s}$. By 3.41 we have that $S_{X,r} \cong S_{Y,s}$ which by definition of C means that $r \in C$ or as $C = S_{X,r}$ that $r < r$ a contradiction. So we have that

$$\neg(C \text{ is a initial segment of } X \wedge D \text{ is a initial segment of } Y) \tag{3.42}$$

As C is a section of X we have by [theorem: 3.83] that

$$X = C \text{ or } C \text{ is a initial segment of } X \tag{3.43}$$

Like wise, as D is a section of Y we have by [theorem: 3.83] that

$$Y = D \text{ or } D \text{ is a initial segment of } Y \tag{3.44}$$

We have taking [eq: 3.43] and [eq: 3.44] in account that either:

$\boldsymbol{X = C \wedge Y = D}$**.** then by [eq: 3.41]

$$X \cong Y$$

Using theorem [theorem: 3.89] and the above we have that

$$X \text{ is not order isomorphic with a sub-class of Y}$$

$$Y \text{ is not order isomorphic with a sub-class of X}$$

$\boldsymbol{X = C \wedge Y \neq D}$**.** then by [eq: 3.44] we have that D is a initial segment of Y, which as by [eq: 3.41] $X = C \cong D$ prove that

$$X \text{ is order isomorphic with a initial segment of } Y$$

If Y is order isomorphic with a initial segment of X then by [theorem: 3.88] we have that X is not order isomorphic to a subset of Y contradicting $X \cong D$ and $X \cong Y$. So

$$Y \text{ is not order isomorphic to } a \text{ initial segment of } X$$

$$X \text{ is not order isomorphic to } Y$$

$\boldsymbol{X \neq C \wedge Y = D}$**.** then by [eq: 3.43] we have that C is a initial segment of X, which as by [eq: 3.41] $C \cong D \underset{\text{[theorem: 3.54]}}{\Rightarrow} Y = D \cong C$ proves that

$$Y \text{ is order isomorphic with a initial segment of } X$$

If X is order isomorphic with a initial segment of Y then by [theorem: 3.88] we have that Y is not order isomorphic to a subset of X contradicting $Y \cong C$ and $Y \cong X$. So

$$X \text{ is not order isomorphic to } a \text{ initial segment of } Y$$

$$X \text{ is not order isomorphic to } Y$$

$\boldsymbol{X \neq C \wedge Y \neq D}$**.** Using [eq: 3.43] and [eq: 3.44] we have that C is a initial segment of X and D is a initial segment of Y which contradicts [eq: 3.42]. Hence this case does not apply. □

Corollary 3.92. *Let $\langle X, \leqslant \rangle$ be a well ordered class and $Y \subseteq X$ then we have either (but not both):*

1. *Y is order isomorphic with X*
2. *X is order isomorphic with a initial segment of X*

Proof. If $Y \subseteq X$ then $\langle Y, \leqslant_{|Y} \rangle$ is a well ordered class [see theorem: 3.78], so using the previous [theorem: 3.91] we have either:

1. Y is order isomorphic with X
2. Y is order isomorphic with a initial segment of X
3. X is order isomorphic with a initial segment of Y. By [theorem: 3.88] we may not have that Y is order isomorphic with a sub-class of X. As by [theorem: 3.54] $Y \cong Y$ and Y is a sub-class of X we reach a contradiction, so this case never applies. □

3.4 Axiom of choice

The axiom of choice in it's many equivalent forms like

$$\text{Hausdorff}'s \, \text{Maximal Principle}$$
$$\text{Zorn}'s \, \text{Lemma}$$
$$\text{Well} - \text{Ordering Theorem}$$

plays a major role in some fundamental theorems about the product of sets, the existence of a basis for a vector space, etc.

Definition 3.93. *Let A be a class then $\mathcal{P}'(A)$ is defined as*

$$\mathcal{P}'(A) = \mathcal{P}(A) \backslash \{\varnothing\}$$

In other words it is the collection of all non empty sub sets of a set

It turns out that if A is a set then $\mathcal{P}'(A)$ is also a set.

Theorem 3.94. *If A is a set then $\mathcal{P}'(A)$ is a set*

Proof. Using the Axiom of Power [axiom 1.64] we have that $\mathcal{P}(A)$ is a set. As $\mathcal{P}'(A) \subseteq \mathcal{P}(A)$ [see [theorem: 1.25] it follow from the Axiom of Subsets [axiom: 1.54] that $\mathcal{P}'(A)$ is a set. □

Definition 3.95. (Choice Function) *Let A be a set then a **choice function for A** is a function $f: \mathcal{P}'(A) \rightarrow A$ such that $\forall B \in \mathcal{P}'(A)$ we have $f(B) \in B$*

So a choice function picks out one element out of each subset of A and the axiom of choice ensures the existence of a choice function for a set.

Axiom 3.96. (Axiom of Choice) *If A is a set then there exist a choice function for A*

As a application of the axiom of choice we have the following theorem

Theorem 3.97. *If $f: A \rightarrow B$ is a surjective function then there exists a injective function $g: B \rightarrow A$ such that $f \circ g = \mathrm{Id}_B$*

Proof. By the axiom of choice there exists a choice function

$$c: \mathcal{P}'(A) \rightarrow A \text{ such that } \forall A \in \mathcal{P}'(A) \text{ we have } c(A) \in A$$

If $f: A \rightarrow B$ is surjective. Then $\forall y \in B$ we have that $f^{-1}(\{y\})$ is a non empty subset of $A \Rightarrow f^{-1}(\{y\}) \in \mathcal{P}'(A)$. Define then the function

$$g: B \rightarrow Y \text{ by } g(y) = c(f^{-1}(\{y\}))$$

Now if $y \in Y$ then, as c is a choice function, $c(f^{-1}(\{y\})) \in f^{-1}(\{y\})$ so that $f(c(f^{-1}(\{y\}))) = y$. Hence we have that $(f \circ g)(y) = f(g(y)) = f(c(f^{-1}(\{y\}))) = y$ or

$$f \circ g = \mathrm{Id}_B$$

If $g(y) = g(y')$ then we have $f(g(y)) = f(g(y')) \underset{f \circ g = \mathrm{Id}_B}{\Rightarrow} \mathrm{Id}_B(y) = \mathrm{Id}_B(y') \Rightarrow y = y'$ proving that

$$g: B \rightarrow Y \text{ is injective}$$ □

The important thing to remember in the above is that the axiom of choice ensures the existence of $g: B \rightarrow A$ but does not give a way to construct the function g itself.

We have the following equivalent statements of the axiom of choice

Theorem 3.98. *The following are equivalent*

1. *The Axiom of Choice*
2. *Let $\mathcal{A}$ be a set of sets such that:*
   a. $\forall A \in \mathcal{A}$ *we have* $A \neq \varnothing$
   b. $\forall A, B \in \mathcal{A}$ *with* $A \neq B$ *we have* $A \bigcap B = \varnothing$

   *then there exist a set C called the **choice set for $\mathcal{A}$** such that*

   a. $C \subseteq \bigcup \mathcal{A}$

b. $\forall A\in\mathcal{A}$ *we have* $A\bigcap C\neq\varnothing$ *and if* $y,y'\in A\bigcap C$ *then* $y=y'$

In other words C *consists of exactly one element from each* $A\in\mathcal{A}$*.*

3. If $\{A_i\}_{i\in I}\subseteq\mathcal{A}$ *is a family of non empty sets [*$\forall i\in I$ *we have* $A_i\neq\varnothing$*] where* $I,\mathcal{A}$ *are sets then there exists a function* $f\colon I\rightarrow\bigcup_{i\in I}A_i$ *such that* $\forall i\in I$ *we have* $f(i)\in A_i$

Proof.

1 $\Rightarrow$ **2.** Take $U=\bigcup\mathcal{A}$ [see definition: 1.56]. As $\mathcal{A}$ is a set we have by the Axiom of Union [axiom: 1.61] that U is a set. So we can apply the Axiom of Choice [axiom: 3.96] to get a function

$$c\colon\mathcal{P}'(U)\rightarrow U \text{ such that } \forall A\in\mathcal{P}'(U) \text{ we have } c(A)\in A$$

If $A\in\mathcal{A}$ then $A\neq\varnothing$ and using [theorem: 1.60] we have $A\subseteq U$ proving that $A\in\mathcal{P}'(U)$ hence

$$\mathcal{A}\subseteq\mathcal{P}'(U)$$

so we can take the **image** of $\mathcal{A}$ by c

$$C=c(\mathcal{A})$$

We have now:

a) If $x\in C$ then $\exists A\in\mathcal{A}$ such that $x=(c)(A)$, which as c is a choice function means that $x\in A$ hence, by [theorem: 1.60], we have that $x\in\bigcup\mathcal{A}$ proving that

$$C\subseteq\bigcup\mathcal{A}$$

b) Let $A\in\mathcal{A}$ then $(c)(A)\in c(\mathcal{A})=C$ and, as c is a choice function, $(c)(A)\in A$ [note: $(c)(A)$ is function application and $c(\mathcal{A})$ is the image of $\mathcal{A}$ by c]. Hence

$$A\bigcap C\neq\varnothing$$

If $y,y'\in A\bigcap C$ then as $y,y'\in C=c(\mathcal{A})$ there exist $Y,Y'\in\mathcal{A}$ such that $y=(c)(Y)$ and $y'=(c)(Y')$, as c is a choice function we have $y=(c)(Y)\in Y$ and $y'=(c)(Y')\in Y'$. Assume that $Y\neq Y'$ then we have the contradiction $y,y'\in Y\bigcap Y'=\varnothing$, so we have that Y=Y' but then $y=c(Y)=c(Y')=y'$ proving that $y=y'$. So

$$y,y'\in A\bigcap C\Rightarrow y=y'$$

so (2.a) and (2.b) is proved.

2 $\Rightarrow$ **1.** Let A be a set and let $B\in\mathcal{P}'(A)$ then $\varnothing\neq B\subseteq A$. Define now

$$P_B=\{(B,x)|x\in B\} \tag{3.45}$$

If $(B,x)\in P_B$ then as $B\in\mathcal{P}'(A)$ and $x\in B\subseteq A$ we have $(B,x)\in\mathcal{P}'(A)\times A$ or

$$P_B\subseteq\mathcal{P}'(A)\times A \text{ or } P_B\in\mathcal{P}(\mathcal{P}'(A)\times A) \tag{3.46}$$

As $B\neq\varnothing$ we have that $\exists b\in B$ so that $(B,p)\in P_B$ proving that

$$\forall B\in\mathcal{P}'(A) \text{ we have } P_B\neq\varnothing \tag{3.47}$$

If $x\in P_B\bigcap P_{B'}$ then $\exists b\in B$ and $b'\in B$ such that $(B,b)=x=(B',b')$ proving that $B=B'$, hence $P_B=P_{B'}$. From this it follows that

$$\forall B,B'\in\mathcal{P}'(A) \text{ we have If } P_B\neq P_{B'} \text{ then } P_B\bigcap P_{B'}=\varnothing \tag{3.48}$$

Define

$$\mathcal{A}=\{P_B|B\in\mathcal{P}'(A)\}\subseteq\mathcal{P}(\mathcal{P}'(A)\times A) \tag{3.49}$$

As A is a set we have by [theorem: 3.94] that $\mathcal{P}'(A)$ is a set, using [theorem: 1.67] it follow that $\mathcal{P}'(A)\times A$ is a set, applying the Axiom of Power sets [axiom: 1.64] proves that $\mathcal{P}(\mathcal{P}'(A)\times A)$ is a set. As by [eq: 3.49] we have that $\mathcal{A}\subseteq\mathcal{P}(\mathcal{P}'(A)\times A)$ we can use the Axiom of Sub Sets [axiom: 1.54] giving

$$\mathcal{A}\,\text{is}\,a\,\text{set} \tag{3.50}$$

So the conditions for the hypothesis (2) are satisfied by [eq: 3.50],[eq: 3.47] and [eq: 3.48] hence there exist a choice set C for $\mathcal{A}$ such that:

$$C\subseteq\bigcup\mathcal{A} \text{ and } \forall B\in\mathcal{A} \text{ we have } B\bigcap C\neq\varnothing \text{ and if } y,y'\in B\bigcap C \text{ then } y=y' \tag{3.51}$$

If $x\in C$ then $\exists y\in\mathcal{A}$ such that $x\in y$. As $y\in\mathcal{A}$ there exists a $B\in\mathcal{P}'(A)$ such that $y=P_B=\{(B,x)|x\in B\}$, hence there exist a $b\in B$ such that $x=(B,b)\in P_B\subseteq\mathcal{P}'(A)\times A$ [see eq: 3.46] proving that

$$C\subseteq\mathcal{P}'(A)\times A \tag{3.52}$$

If $(B,y),(B,y')\in C$ then $(B,y),(B,y')\in P_B\bigcap C \underset{[\text{eq: } 3.51}{\Rightarrow} (B,y)=(B,y')$ proving that $y=y'$, so

$$\text{If } (B,y),(B,y')\in C \text{ then } y=y' \tag{3.53}$$

Let $B\in\mathcal{P}'(A)$ then $P_B\in\mathcal{A}$ so that by [eq: 3.51] $P_B\bigcap C\neq\varnothing$ hence there exist a $y\in B$ such that $(B,y)\in C$ proving that

$$\mathcal{P}'(A)\subseteq\operatorname{dom}(C) \tag{3.54}$$

From [eq: 3.52], [eq: 3.53] and [eq: 3.54] it follows that

$$C:\mathcal{P}'(A)\rightarrow A \text{ is a function} \tag{3.55}$$

Let $B\in\mathcal{P}'(A)$ then $(B,C(B))\in C\subseteq\bigcup\mathcal{A}$ so that $\exists B'\in\mathcal{P}'(A)$ such that $(B,C(B))\in P_{B'}$ hence $B=B'$ and $C(B)\in B'=B$ proving that $\forall B\in\mathcal{P}'(A)$ we have $C(B)\in B$, so that

$$C:\mathcal{P}'(A)\rightarrow A \text{ is a choice function}$$

proving (1)

$1\Rightarrow 3$. Let $\{A_i\}_{i\in I}\subseteq\mathcal{A}$ be a family of non empty sets where $I,\mathcal{A}$ are sets. Then using [theorem: 2.103] it follows that $\bigcup_{i\in I}A_i$ is a set. Using the Axiom of Choice [axiom: 3.96] there exist a choice function

$$c:\mathcal{P}'\left(\bigcup_{i\in I}A_i\right)\rightarrow\bigcup_{i\in I}A_i \text{ where } \forall A\in\mathcal{P}'\left(\bigcup_{i\in I}A_i\right)\ c(A)\in A$$

Let $A:I\rightarrow\mathcal{A}$ be the function that defines $\{A_i\}_{i\in I}\subseteq\mathcal{A}$ then $\forall i\in I$ we have that $A(i)=A_i\subseteq\bigcup_{i\in I}A_i$ [see: theorem: 2.110] or $A(i)\in\mathcal{P}(\bigcup_{i\in I}A_i)$, further as $A_i\neq\varnothing$ we have that $A_i\in\mathcal{P}'(\bigcup_{i\in I}A_i)$, hence $\operatorname{range}(A)\subseteq\mathcal{P}'(\bigcup_{i\in I}A_i)$. Using [theorem: 2.32] it follows that $A:I\rightarrow\mathcal{P}'(\bigcup_{i\in I}A_i)$ is also a function. If we take $f=c\circ A$ then

$$f:I\rightarrow\bigcup_{i\in I}A_i \text{ is a function and } \forall i\in I \text{ we have } f(i)=c(A(i))=c(A_i)\in A_i$$

proving (3).

$3\Rightarrow 1$. Let A be a set and define the family $\{B_C\}_{C\in\mathcal{P}'A}\subseteq\mathcal{P}'(A)$ by $B=\operatorname{Id}_{\mathcal{P}'(A)}:\mathcal{P}'(A)\rightarrow\mathcal{P}'(A)$ [see example: 2.42]. For every $C\in\mathcal{P}'(A)$ we have $B_C=\operatorname{Id}(C)=C\neq\varnothing$, further as A is a set we have by [theorem: 3.94] that $\mathcal{P}'(A)$ is a set. So the conditions for (3) are satisfied and by (3) there exist a function

$$f:\mathcal{P}'(A)\rightarrow\bigcup_{C\in\mathcal{P}'(A)}B_C \text{ such that } \forall C\in\mathcal{P}'(A) \text{ we have } f(C)\in B_C=\operatorname{Id}(C)=C \tag{3.56}$$

Let $x\in\bigcup_{C\in\mathcal{P}'(A)}B_C$ then $\exists C\in\mathcal{P}'(A)$ such that $x\in B_C=\operatorname{Id}_{\mathcal{P}'(A)}(C)=C\subseteq A\Rightarrow x\in A$. So $\bigcup_{C\in\mathcal{P}'(A)}B_C\subseteq A$. Using then [theorem: 2.28] we have

$$f:\mathcal{P}'(A)\rightarrow A \text{ is a function with } \forall C\in\mathcal{P}'(A) \text{ we have } f(C)\in C$$

which proves that $f:\mathcal{P}'(A)\rightarrow A$ is a choice function for A, proving (1). □

As a application of the Axiom of Choice we have the following theorems about the product of a family of sets. First we prove that the projection function is surjective.

Theorem 3.99. *Let $\{A_i\}_{i\in I}\subseteq\mathcal{A}$ be a family of* ***non empty sets*** *where $I,\mathcal{A}$ are sets then $\forall i\in I$ we have that the projection function*

$$\pi_i: \prod_{j\in I} A_j \rightarrow A_i \text{ defined by } \pi_j(x)=x(j) \text{ [see definition: 2.128]}$$

is a surjection.

Proof. Let $i\in I$ and take $x\in A_i$. Consider the family $\{A_j\}_{j\in I\setminus\{i\}}$ [see definition: 2.92] then $\forall j\in I\setminus\{i\}$ we have $A_j\neq\varnothing$. So we can use [theorem: 3.98 (3)] to find a function

$$f: I\setminus\{i\}\rightarrow \bigcup_{j\in I\setminus\{i\}} A_j \text{ such that } \forall j\in I\setminus\{i\} \text{ we have } f(j)\in A_j$$

By the definition of the product of a family of sets we have that

$$f\in\prod_{j\in I\setminus\{i\}} A_j$$

Define now $g: I\rightarrow\bigcup_{j\in I} A_j$ by $g(j)=\left\{\begin{smallmatrix} x \text{ if } j=i \\ f(j) \text{ if } j\in I\setminus\{i\}\end{smallmatrix}\right.$ then by [theorem: 2.127] we have that $g\in\prod_{i\in I} A_i$. Finally by $\pi_i(g)=g(i)=x$ proving surjectivity. □

Second we prove that the product of a family of sets is not empty if and only if every set in the family is non empty.

Theorem 3.100. *Let $\{A\}_{i\in I}\subseteq\mathcal{A}$ be a family of sets where $I,\mathcal{A}$ are sets then we have*

$$\prod_{i\in I} A_i\neq\varnothing \Leftrightarrow \forall i\in I \text{ we have } A_i\neq\varnothing$$

Proof.

- **⇒.** We prove this by contradiction, so assume that $\exists i\in I$ such that $A_i=\varnothing$. As $\prod_{i\in I} A_i\neq\varnothing$ there exists a $x\in\prod_{i\in I} A_i$ such that $\forall j\in I$ $x_j\in A_j$, in particular we would have $x_i\in A_i$ contradicting $A_i=\varnothing$. So we must have that $\forall i\in I$ we have $A_i\neq\varnothing$.
- **⇐.** If $\forall i\in I$ we have $A_i\neq\varnothing$ we have by [theorem: 3.98 (3)] that there exist a function

$$f: I\rightarrow\bigcup_{i\in I} A_i \text{ such that } \forall i\in I \text{ we have } f(i)\in \mathrm{A}_i$$

which by definition of the product means that $f\in\prod_{i\in I} A_i$ proving that

$$\prod_{i\in I} A_i\neq\varnothing$$

□

We can rephrase the above theorem in another way.

Corollary 3.101. *Let $\{A\}_{i\in I}\subseteq\mathcal{A}$ be a family of sets where $I,\mathcal{A}$ are sets then we have*

$$\prod_{i\in I} A_i=\varnothing \Leftrightarrow \exists i\in I \text{ such that } A_i=\varnothing$$

Proof. We proceed by contradiction to prove this

- **⇒.** Assume that $\forall i\in I$ we have that $A_i\neq\varnothing$ then by [theorem: 3.100] $\prod_{i\in I} A_i\neq\varnothing$ contradicting $\prod_{i\in I} A_i=\varnothing$. So the assumption is false or $\exists i\in I$ such that $A_i=\varnothing$.
- **⇐.** Assume that $\prod_{i\in I} A_i\neq 0$ then by [theorem: 3.100] we have $\forall i\in I$ that $A_i\neq\varnothing$ contradicting $\exists i\in I$ such that $A_i=0$. Hence we must have $\prod_{i\in I} A_i=\varnothing$. □

The Axiom of Choice has also import consequences for partial ordered sets.

Theorem 3.102. *Let $\langle X,\leqslant\rangle$ be a partial ordered* ***set*** *such that:*

1. *X has a least element p*

2. *Every chain [see definition:3.39] of X has a supremum*

then there is a element $x \in X$ which has no immediate successor [see definition: 3.80]

Proof. We prove this by contradiction, so assume that $\forall x \in X$ there exist a immediate successor. Given $x \in X$ define $T_x = \{y | y \text{ is a immediate successor of } x\}$ then $T_x \neq \varnothing$ so that $T_x \in \mathcal{P}'(X)$. Using the Axiom of Choice [axiom: 3.96] there exist a choice function

$$c: \mathcal{P}'(A) \rightarrow A \text{ such that } \forall A \in \mathcal{P}'(X) \text{ we have } c(A) \in A \tag{3.57}$$

As $\forall x \in X$ we have $T_x \in \mathcal{P}'(X)$ so that $c(T_x)$ is well defined we can use [proposition: 2.86] to define the function

$$\operatorname{succ}: X \rightarrow X \text{ by } \operatorname{succ}(x) = c(T_x).$$

If $x \in X$ then $\operatorname{succ}(x) = c(T_x) \in T_x$ so that $\operatorname{succ}(x)$ is a immediate successor of x, to summarize

$$\operatorname{succ}: X \rightarrow X \text{ is a function such that } \forall x \in X \ \operatorname{succ}(x) \text{ is a immediate successor of } x \tag{3.58}$$

Before we can reach the contradiction we need to have some definitions and sub lemmas.

Definition 3.103. *$A \subseteq X$ is a **p-sequence** iff*

1. *$p \in A$*
2. *If $x \in A$ then $\operatorname{succ}(x) \in A$*
3. *If $C \subseteq A$ is a chain then $\sup(C) \in A$ [note that by hypothesis (2) $\sup(C)$ exist]*

Note 3.104. X is a p-sequence so there exist p-sequences.

Proof. First $p \in X$ by the hypothesis (1), second if $x \in X$ then by [eq: 3.58] $\operatorname{succ}(X) \in X$ and finally if C is chain then by definition of the supremum $\sup(C) \in X$ □

Lemma 3.105. *Every intersection of a set of p-sequences is a p-sequence*

Proof. Let $\mathcal{A}$ be a set of p-sequences then

1. $\forall A \in \mathcal{A}$ A is a p-sequence hence $p \in A$ so that $p \in \bigcap \mathcal{A}$
2. If $x \in \bigcap \mathcal{A}$ then $\forall A \in \mathcal{A}$ we have $p \in A$ which as A is a p-sequence gives that $\operatorname{succ}(x) \in A$ hence $\operatorname{succ}(x) \in \bigcap \mathcal{A}$
3. If $C \subseteq \bigcap \mathcal{A}$ is a chain then $\forall A \in \mathcal{A}$ we have $C \subseteq A$ and as A is a p-sequence we have that $\sup(C) \in A$ so that $\sup(A) \in \bigcap \mathcal{A}$

so by definition of a p-sequence we have that

$$\bigcap \mathcal{A} \text{ is a p-sequence}$$ □

From the above lemma [lemma: 3.105] we have that $\bigcap \{A \in \mathcal{P}(X) | A \text{ is a p-sequence}\}$ is a p-sequence and by definition $p \in \bigcap \{A \in \mathcal{P}(X) | A \text{ is a p-sequence}\}$. Further if A is a p-sequence then $\bigcap \{A \in \mathcal{P}(X) | A \text{ is a p-sequence}\} \subseteq A$. Summarized

$$P = \bigcap \{B \in \mathcal{P}(X) | B \text{ is a p-sequence }\} \text{ is a p-sequence} \wedge p \in P \wedge \text{If } A \text{ is a p-sequence} \Rightarrow P \subseteq A \tag{3.59}$$

Definition 3.106. *A element $x \in P$ is **select** if x is comparable with every element in P.*

Lemma 3.107. *If $x \in P$ is select then $\forall y \in P$ with $y < x$ have $\operatorname{succ}(y) \leqslant x$*

Proof. If $y \in P$ with $y < x$ then as P is a p-sequence we have by [definition: 3.103 (2)] that $\operatorname{succ}(y) \in P$. Now as x is select we have that $x, \operatorname{succ}(y)$ are comparable, hence by [theorem: 3.37] we have either $\operatorname{succ}(y) \leqslant x$ or $x < \operatorname{succ}(y)$. If $x < \operatorname{succ}(y)$ then from $y < x$ it follows that $y < x \wedge x < \operatorname{succ}(y)$ contradicting the fact that by [eq: 3.58] $\operatorname{succ}(y)$ is the immediate successor of y. Hence we must have that

$$\operatorname{succ}(y) \leqslant x$$ □

Lemma 3.108. *If x is select then $A_x = \{y \in P | y \leqslant x \vee \mathrm{succ}(x) \leqslant y\}$ is a p-sequence*

Proof.

1. As p is a least element of X we have that $p \leqslant x$ so that $p \in A_x$
2. Let $y \in A_x$ Then we have either:

   $y = x$. Then $\mathrm{succ}(x) = \mathrm{succ}(y) \Rightarrow \mathrm{succ}(x) \leqslant \mathrm{succ}(y)$ so that $\mathrm{succ}(y) \in A_x$.

   $y < x$. Then as $y \in A_x \subseteq P$ we have by the previous lemma [lemma: 3.107] that $\mathrm{succ}(y) < x \Rightarrow \mathrm{succ}(y) \leqslant x$ so that $\mathrm{succ}(y) \in A_x$.

   $\mathrm{succ}(x) \leqslant y$. As $\mathrm{succ}(y)$ is the immediate successor of y we have $y < \mathrm{succ}(y)$ so that $\mathrm{succ}(x) < \mathrm{succ}(y) \Rightarrow \mathrm{succ}(x) \leqslant \mathrm{succ}(y)$ proving that $\mathrm{succ}(y) \in A_x$.

   so in all cases we have

   $$\mathrm{succ}(y) \in A_x$$

3. If $C \subseteq A_x$ is a chain then we have the following excluding cases:

   $\exists y \in C$ with $\mathrm{succ}(x) \leqslant y$. Then as $y \leqslant \sup(C)$ we have that $\mathrm{succ}(x) \leqslant \sup(C)$ so that $\sup(C) \in A_x$.

   $\forall y \in C$ we have $\neg(\mathrm{succ}(x) \leqslant y)$. Now $\forall y \in C$ as $y \in C \subseteq A_x$ we have either $y \leqslant x$ or $\mathrm{succ}(y) \leqslant y$. As $\neg(\mathrm{succ}(x) \leqslant y)$ is true we must have $y \leqslant x$ and thus x is a upper bound of C. So by definition of the supremum as the least upper bound of C we must have that $\sup(C) \leqslant x$, hence $\sup(C) \in A_x$

   So in all cases we have

   $$\sup(C) \in A_x$$

From (1),(2) and (3) it follows then that

$$A_x \text{ is a p-sequence}$$ □

Corollary 3.109. *If x is select then $\forall y \in P$ we have $y \leqslant x$ or $\mathrm{succ}(x) \leqslant y$*

Proof. As A_x is a p-sequence by the previous lemma [lemma: 3.108] we have by [eq: 3.59] that $P \subseteq A_x$ and as by definition of A_x $A_x \subseteq P$ it follows that

$$P = A_x$$ □

Lemma 3.110. *The set $\{x \in X | x \text{ is select}\}$ is a p-sequence.*

Proof.

1. As p is a least element of X we have $\forall x \in P$ that $p \leqslant x$ so it is comparable with every element of p, hence p is select, so $p \in \{x \in X | s \text{ is select}\}$.
2. If $x \in \{x \in X | x \text{ is select}\}$ then x is select and by [corollary: 3.109] we have $\forall y \in P$ either:

   $y \leqslant x$. Then as $\mathrm{succ}(x)$ is the immediate successor of x we have $x < \mathrm{succ}(x)$ so that $y < \mathrm{succ}(x) \Rightarrow y \leqslant \mathrm{succ}(x)$ proving that $\mathrm{succ}(x)$ is comparable with y

   $\mathrm{succ}(x) \leqslant y$. Then $\mathrm{succ}(x)$ is comparable with y

   from the above it follows that $\mathrm{succ}(x)$ is comparable with every $y \in P$ hence

   $$\mathrm{succ}(x) \in \{x \in X | x \text{ is selected}\}$$

3. Let $C \subseteq \{x \in X | x \text{ is select}\}$ be a chain. Then as $C \subseteq X$ we have the hypothesis (3) that $\sup(C)$ exist. Then $\forall y \in P$ we have the following possibilities for C:

   $\exists x \in C$ with $y \leqslant x$. Then $x \leqslant \sup(C)$ so that $y \leqslant \sup(C)$ so that $\sup(C)$ is comparable with y

$\forall x\in C$ we have $\neg(y\leqslant x)$. Then given $x\in C$ we have as $C\subseteq\{x\in X|x \text{ is select}\}$ that x is select. By [corollary: 3.109] we have either $y\leqslant x$ which is not allowed or $\mathrm{succ}(x)\leqslant y$. As $\mathrm{succ}(x)$ is a immediate successor of x we have $x<\mathrm{succ}(x)$ so that $x<y$ proving that y is a upper bound of C. Hence $\sup(C)\leqslant y$ proving that $\sup(C)$ is comparable with y

So in all cases we have that $\sup(C)$ is comparable with y proving that $\sup(C)$ is select and thus that $\sup(C)\in\{x\in X|x \text{ is select}\}$

From (1),(2),(3) it follows then that $\{x\in X|x \text{ is select}\}$ is a p-sequence. □

Now for the last corollary in the proof.

Corollary 3.111. *P is a chain*

Proof. As by the previous lemma [lemma: 3.110] $\{x\in X|x \text{ is select}\}$ is a p-sequence it follows from [eq: 3.59] that $P\subseteq\{x\in X|x \text{ is select}\}$. So if $x,y\in P$ then x is select and as $y\in P$ comparable with y, proving that P is a chain. □

We are now finally able to reach a contradiction and prove the theorem. As P is a chain we have by hypothesis (2) that $\sup(P)$ exist. Now as P is a p-sequence [see eq: 3.59] we have by [definition: 3.103 (3)] that $\sup(P)\in P$ and by [definition: 3.103 (2)] that $\mathrm{succ}(\sup(P))\in P$ so that $\mathrm{succ}(\sup(P))\leqslant\sup(P)$. As $\mathrm{succ}(\sup(P))$ is the immediate successor of $\sup(P)$ we have that $\sup(P)<\mathrm{succ}(\sup(P))$. Hence $\sup(P)<\sup(P)$ which is a contradiction. □

This was a long proof but it will be used in the following important theorem.

Definition 3.112. *A partial ordered set $\langle X,\leqslant\rangle$ is **Hausdorff maximal** if there exist a chain C such that if D is a chain with $C\subseteq D$ then $C=D$. In other words C is maximal when using the order relation defined by $\subseteq$.*

We show now that as a consequence of the Axiom of choice every partial ordered set is Hausdorff maximal.

Theorem 3.113. (Hausdorff's Maximal Theorem) *Let $\langle X,\leqslant\rangle$ be a partial ordered set then it is Hausdorff maximal. In other words there exists a chain C such that if D is a chain such that $C\subseteq D$ then $C=D$.*

Proof. Define the set of all chain of X

$$\mathcal{C}=\{A\in\mathcal{P}(X)|A \text{ is a chain in } \langle X,\leqslant\rangle\}$$

Using the fact $\mathcal{P}(X)$ is a set by the Axiom of Power Sets [axiom: 1.64] we have by the Axiom of Subsets [axiom: 1.54] and the fact that $\mathcal{C}\subseteq\mathcal{P}(X)$ it follows that

$$\mathcal{C} \text{ is a set} \tag{3.60}$$

Using [example: 3.32] we have that

$$\langle\mathcal{C},\preccurlyeq\rangle \text{ where } \preccurlyeq=\{(x,y)\in\mathcal{C}\times\mathcal{C}|x\subseteq y\} \text{ is a partial ordered set}$$

As $\forall A\in\mathcal{C}$ we have $\varnothing\subseteq A\Rightarrow\varnothing\preccurlyeq A$ and $\varnothing$ is a chain [see example: 3.40] in $\langle X,\leqslant\rangle$ it follows that

$$\mathcal{C} \text{ has a least element [using } \preccurlyeq] \tag{3.61}$$

Let $\mathcal{D}$ a chain in $\langle\mathcal{C},\preccurlyeq\rangle$ then if $x,y\in\bigcup\mathcal{D}$ there exists $A,B\in\mathcal{D}\subseteq\mathcal{C}$ such that $x\in A\wedge y\in B$ where A,B are chains in $\langle X,\leqslant\rangle$. As $\mathcal{D}$ is a chain we have either:

$A\subseteq B$. Then $x,y\in B$ which as B is a chain [using $\leqslant$] means that x,y are comparable [using the order $\leqslant$]

$B\subseteq A$. Then $x,y\in A$ which as A is a chain [using $\leqslant$] means that x,y are comparable [using the order $\leqslant$]

From the above it follows that $\bigcup \mathcal{D}$ is a chain in $\langle X, \leqslant\rangle$ hence $\bigcup \mathcal{D} \in \mathcal{C}$. Hence by [example: 3.66] it follows that $\bigcup \mathcal{D} = \sup(\mathcal{D})$ [using $\preccurlyeq$]. So we have proved that

$$\text{Every chain of } \langle \mathcal{C}, \preccurlyeq\rangle \text{ has a supremum} \tag{3.62}$$

Now the conditions for [theorem: 3.102] are satisfied by [eq: 3.60], [eq: 3.61] and [eq: 3.62] so we have

$$\exists C \in \mathcal{C} \text{ [so } C \text{ is a chain in } \langle X, \leqslant\rangle] \text{ which has no immediate successor [using} \preccurlyeq] \tag{3.63}$$

Let now D be a chain in $\langle X, \leqslant\rangle$ [so that $D \in \mathcal{C}$] such that $C \subseteq D$. Take $d \in D$ and assume that $d \notin C$ then $C \subset C \bigcup \{d\}$ [as $C \bigcup \{d\} \nsubseteq C \Rightarrow C \neq C \bigcup \{d\}$] so that $C \prec C \bigcup \{d\}$. As C has no immediate successor [using $\prec$] there must be a $H \in \mathcal{C}$ such that $C \prec H \wedge H \prec C \bigcup \{d\}$ or $C \subset H \wedge H \subset C \bigcup \{d\}$. As $C \subset H$ there exists a $h \in H$ such that $h \notin C$, but then as $H \subset C \bigcup \{d\}$ we must have $h \in \{d\}$ or $h = d$, so $d \in H$. Now as $H \subset C \bigcup \{d\}$ there exists a $y \in C \bigcup \{d\}$ such that $y \notin H$, we can not have $y = d$ [as $d \in H$] so we must have $y \in C$ but then as $C \subset H$ we have $y \in H$ contradicting $y \in H$. So we must have $d \in C$. As $d \in D$ was chosen arbitrary we have that $D \subseteq C$ or $C = D$ which proves maximality. □

We state now Zorn's lemma but not prove it yet, it will be show to be directly dependent on the Hausdorff maximal principle, which in turn depends on the Axiom of Choice. So if we accept the Axiom of Choice [which we do as it is a expressed as a Axiom] then Zorn's lemma applies.

Lemma 3.114. (Zorn's Lemma) *Let $\langle X, \leqslant\rangle$ be a partial ordered set such that every chain has a upper bound then X has a maximal element.*

We prove now that the Hausdorff Maximal principle implies Zorn's lemma.

Theorem 3.115. *Let $\langle X, \leqslant\rangle$ be Hausdorff Maximal then Zorn's lemma follows.*

Proof. Let $\langle X, \leqslant\rangle$ be a partial ordered set such that every chain in X has a upper bound. As $\langle X, \leqslant\rangle$ is Hausdorff maximal [definition: 3.112] there exist a chain C such that for every chain D with $C \subseteq D$ we have $C = D$. As C is a chain it has by the hypothesis a upper bound u for C. Assume now that u is not a maximal element of X, then by the definition of a maximal element [definition: 3.56] there exist a $x \in X$ with $u \leqslant x$ and $u \neq x$ so that $u < x$. If $x \in C$ then as u is a upper bound of C we have $x \leqslant u$ so that $u < u$ a contradiction. So we must have that $x \notin C$. Consider now $r, s \in C \bigcup \{x\}$ then we have to consider the following possibilities:

- $\boldsymbol{r = x \wedge s = x}$**.** Then by reflectivity we have $r \leqslant s$, so r, s are comparable.
- $\boldsymbol{r = x \wedge s \neq x}$**.** Then $s \in C$ so that $s \leqslant u$, which as $u \leqslant x$ proves that $s \leqslant x \underset{r=x}{\Rightarrow} s \leqslant r$, so r, s are comparable.
- $\boldsymbol{r \neq x \wedge s = x}$**.** Then $r \in C$ so that $r \leqslant u$, which as $u \leqslant x$ proves that $r \leqslant x \underset{s=x}{\Rightarrow} r \leqslant s$, so r, s are comparable.
- $\boldsymbol{r \neq x \wedge s \neq x}$**.** Then $r, s \in C$, which as C is a chain proves that r, s are comparable

From the above it follows that $C \bigcup \{x\}$ is a chain such that $C \subseteq C \bigcup \{x\}$ giving by maximality of C that $C = C \bigcup \{x\}$ contradicting $x \notin C$. Hence the assumption that u is not a maximal element of X is false. So u is a maximal element of X. □

We show now that Zorn's lemma implies well ordering.

Theorem 3.116. *Zorn's lemma implies that given a set X there exist a order relation $\leqslant$ on X such that $\langle X, \leqslant\rangle$ is well ordered [see 3.77]*

Proof. Just like the proof of [theorem: 3.102] this proof will consist of many sub lemma's.

Let X be a set and define the class

$$\mathcal{A} = \{(B, R) | B \in \mathcal{P}(A) \wedge R \text{ a order relation on } B \text{ so that } \langle B, R\rangle \text{ is well ordered}\}$$

Define now $\preccurlyeq \in \mathcal{A}\times\mathcal{A}$ by

$$\preccurlyeq = \{((B,R),(B',R'))|B\subseteq B'\wedge R\subseteq R'\wedge \text{If } x\in B\wedge y\in B'\backslash B \text{ then } (x,y)\in R'\}$$

then we have that

$$\langle\mathcal{A},\preccurlyeq\rangle \text{ is a order relation} \tag{3.64}$$

Proof. We have to prove reflexivity, anti-symmetry and transitivity:

reflectivity. If $(B,R)\in\mathcal{A}$ then we have

1. $B\subseteq B$
2. $R\subseteq R$
3. If $x\in B\wedge y\in B\backslash B \underset{[\text{theorem: } 1.32]}{=} \varnothing$ which can not occur so that $(x,y)\in R$ is satisfied vacuously

proving that $(B,R)\preccurlyeq(B,R)$

anti-symmetry. If $(B,R)\preccurlyeq(B',R')\wedge(B',R')\preccurlyeq(B,R)$ then $B\subseteq B'\wedge R\subseteq R'\wedge B'\subseteq B\wedge R'\subseteq R$ proving that $B=B'$ and $R=R'$ so that $(B,R)=(B',R')$

transitivity. Let $(B,R)\preccurlyeq(B',R')$ and $(B',R')\preccurlyeq(B'',R'')$ then we have

1. $B\subseteq B'\wedge B'\subseteq B''\Rightarrow B\subseteq B''$
2. $R\subseteq R'\wedge R'\subseteq R''\Rightarrow R\subseteq R''$
3. If $x\in B\wedge y\in B''\backslash B$ we have for y to consider the following possibilities

   $\boldsymbol{y\in B'}$**.** Then $y\in B'\backslash B$ so that $(x,y)\in R' \underset{R'\subseteq R''}{\Rightarrow} (x,y)\in R''$

   $\boldsymbol{y\notin B'}$**.** Then $y\in B''\backslash B'$ so that $(x,y)\in R''$

   so in all cases we have $(x,y)\in R''$.

proving $(B,R)\preccurlyeq(B'',R'')$. □

We now have the following sub lemma:

Lemma 3.117. *If $\mathcal{C}\subseteq\mathcal{A}$ is a chain in $\langle\mathcal{A},\preccurlyeq\rangle$ then if*

$$B_{\mathcal{C}} = \bigcup\{B|\exists R \textit{ such that } (B,R)\in\mathcal{C}\}$$

$$R_{\mathcal{C}} = \bigcup\{R|\exists B \textit{ such that } (B,R)\in\mathcal{C}\}$$

then

$$(B_{\mathcal{C}},R_{\mathcal{C}})\in\mathcal{A}$$

Proof. First note that if $(B,R)\in\mathcal{C}$ then

$$B\in\{B|\exists R \text{ such that } (B,R)\in\mathcal{C}\}$$

and

$$R\in\{R|\exists B \text{ such that } (B,R)\in\mathcal{C}\}$$

or

$$\forall(B,R)\in\mathcal{C} \text{ we have } B\subseteq B_{\mathcal{C}}\wedge R\subseteq R_{\mathcal{C}} \tag{3.65}$$

1. If $x\in B_{\mathcal{C}}$ then $\exists(B,R)\in\mathcal{C}$ such that $x\in B$, as $\mathcal{C}\subseteq\mathcal{A}$ we have $(B,R)\in\mathcal{C}$, so that $B\in\mathcal{P}(A)$, hence $B\subseteq A$, proving that $x\in A$. In other words $B_{\mathcal{C}}\subseteq A$ or $B\in\mathcal{P}(A)$.
2. We must prove that $R_{\mathcal{C}}$ is a a order relation on $B_{\mathcal{C}}$:

   reflectivity. If $x\in B_{\mathcal{C}}$ then $\exists(B,R)\in\mathcal{C}$ such that $x\in B$, as R is a order relation we have that $(x,x)\in R$ so that by [eq: 3.65] $(x,x)\in R_{\mathcal{C}}$

anti-symmetry. If $(x, y) \in R_{\mathcal{C}} \wedge (y, x) \in R_{\mathcal{C}}$ then $\exists (B, R), (B', R') \in \mathcal{C}$ such that $(x, y) \in R$ and $(y, x) \in R'$. As $\mathcal{C}$ is a chain we have either:

$(B, R) \preccurlyeq (B', R')$. Then $R \subseteq R'$ so that $(x, y) \in R' \wedge (y, x) \in R'$, which as R' is a order relation proves that $x = y$.

$(B', R') \preccurlyeq (B, R)$. Then $R' \subseteq R$ so that $(x, y) \in R \wedge (y, x) \in R$, which as R is a order relation proves that $x = y$.

transitivity. If $(x, y) \in R_{\mathcal{C}} \wedge (y, z) \in R_{\mathcal{C}}$ then $\exists (B, R), (B', R') \in \mathcal{C}$ such that $(x, y) \in R$ and $(y, x) \in R'$. As $\mathcal{C}$ is a chain we have either:

$(B, R) \preccurlyeq (B', R')$. Then $R \subseteq R'$ so that $(x, y) \in R' \wedge (y, z) \in R'$, which as R' is a order relation proves that $(x, z) \in R'$, hence $(x, z) \in R_{\mathcal{C}}$ [see eq: 3.65].

$(B', R') \preccurlyeq (B, R)$. Then $R' \subseteq R$ so that $(x, y) \in R \wedge (y, z) \in R$, which as R is a order relation proves that $(x, z) \in R$, hence $(x, z) \in R_{\mathcal{C}}$ [see eq: 3.65].

3. Next we have to prove well ordering of $\langle B_{\mathcal{C}}, R_{\mathcal{C}} \rangle$. Let $D \subseteq B_{\mathcal{C}}$ and $D \neq \varnothing$. Then there exist a $x \in D$ so that $x \in B_{\mathcal{C}}$, hence there exist a $(B, R) \in \mathcal{C}$ such that $x \in B$ or $x \in D \bigcap B$ proving that $D \bigcap B \neq \varnothing$. As $\mathcal{C} \subseteq \mathcal{A}$ we have by the definition of $\mathcal{A}$ that $\langle B, R \rangle$ is well ordered, hence there exist a least element $b \in B$. So

$$\forall y \in B \text{ we have } (b, y) \in R \tag{3.66}$$

We prove now that

$$b \text{ is a least element of } D$$

Proof. If $x \in D$ then $\exists (B', R')$ such that $x \in B'$. For x and B we the following possible cases:

$x \in B$. Then by [eq: 3.66] we have that $(b, x) \in R$ so that by [eq: 3.65] $(b, x) \in R_{\mathcal{C}}$.

$x \notin B$. Then $x \in B' \setminus B \wedge b \in B$. As $\mathcal{C}$ is a chain we have the following cases:

$(B, R) \preccurlyeq (B', R')$. Then by definition of $\preccurlyeq$ we have $(b, x) \in R'$ so that by [eq: 3.65] $(b, x) \in R_{\mathcal{C}}$

$(B', R') \preccurlyeq (B, R)$. Then $B' \subseteq B$ and as $x \in B'$ we have $x \in B$ contradicting $x \notin B$. So this case never occurs.

So in all cases that apply we have $(b, x) \in R_{\mathcal{C}}$ proving that b is a least element of D. □

As we have proved that every non empty $D \subseteq B_C$ has a least element [using the order $R_{\mathcal{C}}$ it follows that $\langle B_{\mathcal{C}}, R_{\mathcal{C}} \rangle$ is well ordered.

From (1),(2) and (3) it follows that

$$(B_{\mathcal{C}}, R_{\mathcal{C}}) \in \mathcal{A}$$ □

Lemma 3.118. *If $\mathcal{C}$ is a chain in $\langle \mathcal{A}, \preccurlyeq \rangle$ then $(B_{\mathcal{C}}, R_{\mathcal{C}})$ is a upper bound of $\mathcal{C}$*

Proof. Let $(B, R) \in \mathcal{C}$ then

1. $B \subseteq B_{\mathcal{C}}$ [see eq: 3.65]
2. $R \subseteq R_{\mathcal{C}}$ [see eq: 3.65]
3. Let $x \in B$ and $y \in B_{\mathcal{C}} \setminus B$ then $\exists (B', R') \in \mathcal{C}$ such that $y \in B'$ or as $y \in B_{\mathcal{C}} \setminus B$ that

$$y \in B' \setminus B$$

As $\mathcal{C}$ is a chain we have either $(B, R) \preccurlyeq (B', R')$ or $(B', R') \preccurlyeq (B, R)$. If $(B', R') \preccurlyeq (B, R)$ then $B' \subseteq B$, as $y \in B'$ we would have $y \in B$ contradiction $y \in B_{\mathcal{C}} \setminus B$. So we have

$$(B, R) \preccurlyeq (B', R')$$

As $x \in B$ and $y \in B' \setminus B$ we have by definition of $\preccurlyeq$ and the above that $(x, y) \in R'$ which as $R' \subseteq R_C$ [see eq: 3.65] proves that $(x, y) \in R_{\mathcal{C}}$

So by the definition of $\preccurlyeq$ we have by (1),(2) and (3) that

$$(B, R) \preccurlyeq (B_{\mathcal{C}}, R_{\mathcal{C}}) \qquad \square$$

Using Zorn's [lemma: 3.114] together with the above lemma [lemma: 3.118] we have

$$\exists (B_m, R_m) \in \mathcal{A} \text{ such that } (B_m, R_m) \text{ is a maximum element of } \mathcal{A} \tag{3.67}$$

We prove now by contradiction that

$$B_m = X$$

Proof. Assume that $X \neq B_m$. Then as $B_m \in \mathcal{P}(X) \Rightarrow B_m \subseteq X$ there exist a

$$x \in X \setminus B_m \Rightarrow x \notin B_m.$$

Define

$$R^* = R_m \bigcup \{(b, x) | b \in B_m\} \bigcup \{(x, x)\} \tag{3.68}$$

Then if $(r, s) \in R_m \bigcap \{(b, x) | b \in B_m\}$ we have as $R_m \subseteq B_m \times B_m$ that $s \in B_m \wedge s = x \notin B_m$ a contradiction, if $(r, s) \in R_m \bigcap \{(x, x)\}$ then $r \in B_m \wedge r = x \notin B_m$ a contradiction and finally if $(r, s) \in \{(b, x) | b \in B_m\} \bigcap \{(x, x)\}$ then $r \in B_m \wedge r = x \notin B_m$ a contradiction. So we have

$$R_m \bigcap \{(b, x) | b \in B_m\} = \varnothing \wedge R_m \bigcap \{(x, x)\} = \varnothing \wedge \{(b, x) | b \in B_m\} \bigcap \{(x, x)\} = \varnothing \tag{3.69}$$

Further if $(x, r) \in R^\star$ then we have either $(x, r) \in R_m \Rightarrow x \in B_m$ contradicting $x \notin B_m$, $(x, r) \in \{(b, x) | b \in B_m\} \Rightarrow x \in B_m$ contradicting $x \notin B_m$ or $(x, r) \in \{(x, x)\} \Rightarrow r = x$. To summarize we have

$$\text{If } (x, r) \in R^* \text{ then } r = x \tag{3.70}$$

We prove now that $\langle B_m \bigcup \{x\}, R^* \rangle$ is well ordered.

Proof. First we have:

reflexivity. If $r \in B_m \bigcup \{x\}$ then we have either:

$r \in B_m$. Then as $\langle B_m, R_m \rangle$ is a partial order we have $(r, r) \in R_m \subseteq R^*$.

$r \notin B_m$. Then $r \in \{x\}$ so that $r = x$ hence $(r, r) = (x, x) \in \{(x, x)\} \subseteq R^*$

proving that $(r, r) \in R^*$.

anti-symmetry. If $(r, s) \in R^*$ and $(s, r) \in R^*$ then we have by [eq: 3.68] for (r, s) either:

$(r, s) \in R_m$. Then as $R_m \subseteq B_m \times B_m$ we have $r, s \in B_m$ so that $r \neq x \neq s$ so that $(s, r) \in R_m$ [if $(s, r) \in \{(b, x) | b \in B\} \bigcup \{(x, x)\}$ then $r = x$ contradicting $r \neq x$], which as $\langle B_m, R_m \rangle$ is a partial order gives that $r = s$.

$(r, s) \in \{(b, x) | b \in B_m\}$. Then $s = x$ so that $(x, r) = (s, r) \in R^* \underset{\text{[eq: 3.70]}}{\Rightarrow} r = x = s$ hence $s = r$.

$(r, s) \in \{(x, x)\}$. Then $r = x = s \Rightarrow r = s$.

proving $r = s$

transitivity. If $(r, s) \in R^* \wedge (s, t) \in R^*$ then we have by [eq: 3.68] that:

$(r, s) \in R_m$. We have the following case for (s, t):

$(s, t) \in R_m$. Then as $\langle B_m, R_m \rangle$ is a partial ordered we have $(r, t) \in R_m \subseteq R^*$.

$(s, t) \in \{(b, x) | b \in B_m\}$. Then $t = x$ and $r \in B_m$ so that $(r, t) \in \{(b, x) | b \in B_m\} \subseteq R^*$.

$(s, t) \in \{(x, x)\}$. Then $t = x$ and $r \in B_m$ so that $(r, t) \in \{(b, x) | x \in B_m\} \subseteq R^*$.

$(r, s) \in \{(b, x) | b \in B_m\}$. Then $s = x$ so that $(s, t) = (x, t) \in R^* \underset{\text{[eq: 3.70]}}{\Rightarrow} t = x$. As $r \in B_m$ we have $(r, t) \in \{(b, x) | b \in B_m\} \subseteq R^*$.

$(r,s)\in\{(x,x)\}$. Then $r=x\wedge t=x$ so that $(x,t)=(s,t)\in R^{*}\underset{\text{[eq: 3.70]}}{\Rightarrow} t=x$ hence $(r,t)=(x,x)\in\{(x,x)\}\subseteq R^{\star}$.

proving $(r,t)\in R^{*}$.

Hence

$$\left\langle B_m\bigcup\{x\},R^{*}\right\rangle \text{ is partial ordered}$$

If $\varnothing\neq C\subseteq B_m\bigcup\{x\}$ is non empty then we have for $C\bigcap B_m$ the following possibilities:

$C\bigcap B_m\neq\varnothing$. Then as $\varnothing\neq C\bigcap B_m\subseteq B_m$ and $\langle B_m,R_m\rangle$ is well ordered [see definition of $\mathcal{A}$] there exist a least element $l\in C\bigcap B_m$ so

$$\forall r\in C\bigcap B_m \text{ we have } (l,r)\in R_m \tag{3.71}$$

Now if $r\in C$ we have either:

$r\in B_m$. then $r\in C\bigcap B_m$ so that by the above [eq: 3.71] $(l,r)\in R_m\subseteq R^{*}$

$r\notin B_m$. then as $C\subseteq B_m\bigcup\{x\}$ we have $r=x$ so $(l,r)\in\{(b,x)|b\in B_m\}\bigcup\{(x,x)\}\subseteq R^{*}$

proving that $(l,r)\in R^{*}$. Hence

$$C \text{ has a least element[using } \left\langle B\bigcup\{x\},R^{*}\right]$$

$C\bigcap B_m=\varnothing$. Then $C=\{x\}$ so that $\forall r\in C$ we have $r=x$ so that $(r,x)=(x,x)\in\{(x,x)\}\subseteq R^{*}$ proving that x is a least element of C.

So in all cases we have that C has a least element, hence

$$\left\langle B_m\bigcup\{x\},R^{*}\right\rangle \text{ is well ordered} \qquad \Box$$

Now as $B_m\bigcup\{x\}\subseteq X$, we have by the definition of $\mathcal{A}$ and the above that

$$\left(B_m\bigcup\{x\},R^{*}\right)\in\mathcal{A}$$

Next we have:

1. $B_m\subseteq B_m\bigcup\{x\}$
2. $R_m\subseteq R^{*}$
3. If $r\in B_m$ and $s\in(B_m\bigcup\{x\})\setminus B_m$ then $s=x$ so that $(r,s)=(r,x)\in\{(b,x)|b\in B_m\}\subseteq R^{*}$

proving that $(B_m,R_m)\preccurlyeq(B_m\bigcup\{x\},R^{*})$. As (B_m,R_m) is a maximal element of $\langle\mathcal{A},\preccurlyeq\rangle$ we must have $(B_m,R_m)=(B_m\bigcup\{x\},R^{*})$ so that $B=B\bigcup\{x\}$ which as $x\notin B_m$ leads to a contradiction. Hence the assumption that $X\neq B_m$ is wrong and we must have that

$$X=B_m \qquad \Box$$

As $\langle B_m,R_m\rangle$ is a well ordered the above proves that there exists a partial order R_m such that

$$\langle X,R_m\rangle=\langle B_m,R_m\rangle \text{ is well-ordered [by definition of } \mathcal{A}\ B_m \text{ is well ordered]} \qquad \Box$$

We show now that Well Ordering implies the Axiom of Choice.

Theorem 3.119. *Assume that for every X there exist a order relation such that $\langle X,\leqslant\rangle$ is well ordered then there exists a function $c:\mathcal{P}'(X)\rightarrow X$ such that $\forall A\in\mathcal{P}'(X)$ we have $c(A)\in A$ (Axiom of Choice).*

Proof. Let X be a set then by the hypothesis there exist a order $\leqslant$ on X such that $\langle X,\leqslant\rangle$ is well ordered. Define now $c=\{(A,x)|A\in\mathcal{P}'(X)\wedge x \text{ is a least element of } A\}$. If $(A,x)\in c$ then $A\in\mathcal{P}'(X)$ and x is a least element of A, so that $x\in A\subseteq X$ proving that $(A,x)\in\mathcal{P}'(X)\times X$. So $c\subseteq\mathcal{P}'(X)\times X$. If $(A,x),(A,x')\in c$ then x and x' are least elements of A, which are unique by [theorem: 3.60] so that $x=x'$. Hence we have that

$$c:\mathcal{P}'(X)\rightarrow X \text{ is a partial function}$$

If $A \in \mathcal{P}'(X)$ then $A \neq \varnothing$ so by well ordering A has a least element l so that $(A, l) \in c$, so $\mathcal{P}'(A) \subseteq \operatorname{dom}(c)$. Hence by [proposition: 2.22] we have that

$$c: \mathcal{P}'(X) \rightarrow X \text{ is a function}$$

If $(A, x) \in c$ then x is the least element of A so that $c(A) = x \in A$ proving that

$$c: \mathcal{P}'(X) \rightarrow X \text{ is a choice function for } X$$

□

We are now ready to specify the different equivalent statements of the Axiom of Choice

Theorem 3.120. *The following statements are equivalent*

1. *Axiom of Choice*
2. *Hausdorff's Maximal Principle*
3. *Zorn's Lemma*
4. *Every set can be well ordered*

Proof.

1 ⇒ 2. This follows from [theorem: 3.113]

2 ⇒ 3. This follows from [theorem: 3.115]

3 ⇒ 4. This follows from [theorem: 3.116]

4 ⇒ 1. This follows from [theorem: 3.119] □

As in most of works about mathematics we assume the Axiom of Choice. To summarize the consequences of the Axiom of Choice we have [taking in account [theorem: 3.98] that the following statements are true.

Theorem 3.121.

Axiom of Choice. *Let X be a set then there exist a function $c: \mathcal{P}'(X) \rightarrow X$ such that $\forall A \in \mathcal{P}'(X)$ we have $c(A) \in A$.*

Existence of Choice set. *Let $\mathcal{A}$ be a set of sets such that*

a) $\forall A \in \mathcal{A}$ we have $A \neq \varnothing$

b) $\forall A, B \in \mathcal{A}$ with $A \neq B$ we have $A \bigcap B = \varnothing$

*then there exist a set C [called the **choice set of $\mathcal{A}$**] such that*

a) $C \subseteq \bigcup \mathcal{A}$

b) $\forall A \in \mathcal{A}$ we have $A \bigcap C \neq \varnothing$ and if $y, y' \in A \bigcap C$ then $y = y'$

Axiom of Choice alternative. *If $\{A_i\}_{i \in I} \subseteq \mathcal{A}$ is a family of non empty sets [$\forall i \in I$ we have $A_i \neq \varnothing$] where $I, \mathcal{A}$ are sets then there exists a function $f: I \rightarrow \bigcup_{i \in I} A_i$ such that $\forall i \in I$ we have $f(i) \in A_i$*

Hausdorff's Maximal Theorem. *If $\langle X, \leqslant \rangle$ is a partial ordered set then there exists a chain $C \subseteq X$ such that for every chain $D \subseteq X$ with $C \subseteq D$ we have $C = D$*

Zorn's Lemma. *If $\langle X, \leqslant \rangle$ is a partial ordered set such that every chain has a upper bound then X has a maximal element.*

Well-Ordering Theorem. *For every set there exists a order relation making $\langle X, \leqslant \rangle$ well-ordered.*

There is a kind of extension of Zorn's lemma to pre-ordered sets if change the definition of maximal element slightly.

Theorem 3.122. *Let $\langle X, \leqslant \rangle$ be a pre-ordered set [see definitions: 3.25, 3.24] such that every chain has a upper bound then there exists a $m \in X$ such that $\forall x \in X$ with $m \leqslant x$ we have $x \leqslant m$*

Proof. Using [theorem: 3.33] we have the following

1. $\sim \subseteq X \times X$ defined by $\sim = \{(x, y) \in X | x \leqslant y \wedge y \leqslant x\}$ is a equivalence relation
2. Define $\preccurlyeq \subseteq (X/\sim) \times (X/\sim)$ by

$$\preccurlyeq = \{(x, y) \in (X/\sim) \times (X/\sim) | \exists x' \in \sim[x] \text{ and } \exists y' \in \sim[y] \text{ such that } x' \leqslant y'\}$$

then $\preccurlyeq$ is a order relation in $X/\sim$. So $\langle X/\sim, \preccurlyeq \rangle$ is a partial ordered set

3. $\forall x, y \in A$ we have $x \leqslant y \Leftrightarrow \sim[x] \preccurlyeq \sim[y]$

Let $C \subseteq X/\sim$ be a chain [using the order $\preccurlyeq$] and construct $C' = \bigcup C$. If $x, y \in C'$ then $\exists \sim[x']$, $\sim[y']$ such that $x \in \sim[x']$ and $y \in \sim[y']$, so $x \sim x'$ and $y \sim y'$ or $x \leqslant x' \wedge x' \leqslant x$ and $y \leqslant y' \wedge y' \leqslant y$. As C is a chain [using $\preccurlyeq$] we have the following possibilities:

$\sim[x'] \preccurlyeq \sim[y']$. then $x' \leqslant y'$ and as $x \leqslant x'$ and $y' \leqslant y$ we have $x \leqslant y$

$\sim[y'] \preccurlyeq \sim[x']$. then $y' \leqslant x'$ and as $y \leqslant y'$ and $x' \leqslant x$ we have $y \leqslant x$

proving that x, y are comparable. Hence

$$C' \text{ is a chain [using } \leqslant]$$

By the hypothesis we have that there exist a upper bound u of C' [using $\leqslant$], in other words

$$\exists u \in X \text{ such that } \forall x \in C' \text{ we have } x \leqslant u$$

Take now $\sim[z] \in C$ then $z \in \sim[z] \subseteq C'$ so that $z \leqslant u$ and thus by (3) $\sim[z] \preccurlyeq \sim[u]$. So $\sim[u]$ is a upper bound of C. As we just have proved that every chain in $X/\sim$ has a upper bound and $\langle X/\sim, \preccurlyeq \rangle$ is a partial order, it follows from Zorn's lemma that there exist a maximal element $\sim[m]$ in $X/\sim$. So by [definition: 3.56] we have

$$\forall \sim[x] \in X/\sim \text{ with } \sim[m] \preccurlyeq \sim[x] \text{ we have } \sim[x] = \sim[m]$$

If now $x \in X$ such that $x \leqslant m$ then by (3) we have $\sim[x] \preccurlyeq \sim[m]$ hence by the above we have $\sim[x] = \sim[m]$ so that $x \sim m$ hence $x \leqslant m$. □

As a interesting application of the Axiom of Choice we prove that every function can be restricted to a injection or bijection.

Theorem 3.123. *Let X, Y be sets, $f: X \rightarrow Y$ a function then there exist a $Z \subseteq X$ such that:*

1. *$f_{|Z}: Z \rightarrow Y$ is a injection*
2. *$f_{|Z}(X) = f(X)$*
3. *$f_{|Z}: Z \rightarrow f(X)$ is a bijection*

Proof.

1. Define

$$\mathcal{A} = \{f^{-1}(\{y\}) | y \in f(X)\}.$$

If $A \in \mathcal{A}$ then $\exists y \in f(X)$ such that $A = f^{-1}(\{y\}) \subseteq X$ and as $y \in f(X)$ there exists a $x \in X$ such that $f(x) = y \in \{y\} \Rightarrow x \in f^{-1}(\{y\}) = A$, proving that $A \neq \varnothing$. So we have proved that

$$\mathcal{A} \subseteq \mathcal{P}'(X)$$

By the Axiom of Choice [axiom: 3.96] there exist a function

$$c: \mathcal{P}'(X) \rightarrow X \text{ such that } \forall A \in \mathcal{P}'(X)\ (c)(A) \in A$$

Take

$$Z = c(\mathcal{A}) \subseteq X$$

and consider the restriction of f to Z

$$f_{|Z}: Z \rightarrow Y$$

Let $x, y \in Z$ such that $f_{|Z}(x) = f_{|Z}(y) \underset{x,y \in Z}{\Rightarrow} f(x) = f(y)$. As $x, y \in Z = c(\mathcal{A})$ there exists $A_x \in \mathcal{A} \wedge A_y \in \mathcal{A}$ such that $x = (c)(A_x) \in A_x$ and $y = (c)(A_y) \in A_x$. As $A_x, A_y \in \mathcal{A}$ there exist $x', y' \in f(X)$ such that $A_x = f^{-1}(\{x'\})$ and $A_y = f^{-1}(\{y'\})$. Then $f(x) \underset{x \in A_x}{=} x'$ and $f(y) \underset{y \in A_y}{=} y'$. As $f(x) = f(y)$ we have $x' = y'$ so that $A_x = f^{-1}(\{x'\}) = f^{-1}(\{y'\}) = A_y$. So $x = (c)(A_x) = (c)(A_y) = y$, proving that $x = y$.

2. If $y \in f(X)$ then $f^{-1}(\{y\}) \in \mathcal{A}$ so to that x$=(c)(f^{-1}(\{y\})) \in c(\mathcal{A}) = Z$. Further as $(c)(f^{-1}(\{y\})) \in f^{-1}(\{y\})$ we have that $f(x) = f((c)(f^{-1}(\{y\}))) \in \{y\}$ so that $y = f(x) \in f(Z)$, proving that $f(X) \subseteq f(Z)$. As $Z \subseteq X$ we have by [theorem: 2.15] that $f(Z) \subseteq f(X)$ so that

$$f(X) = f(Z)$$

3. From (2) we have that $f_{|Z}: Z \rightarrow f(X)$ is surjective which together with (1) proves bijectivity. □

From this point on we will gradually start to use the simpler notations for functions and families that are mentioned in the references [definition: 2.34], [theorem: 2.36], [theorem: 2.37], [theorem: 2.48], [theorem: 2.86], [notation: 2.87], [theorem: 2.101] and [theorem: 2.106] without explicit referring to them. This to avoid excessive notation and difference of notation between this text and standard mathematical practice. Another simplification of natation that we introduce is the following.

Notation 3.124. *If $f: A \times B \rightarrow C$ is a function then $f((x, y))$ is noted as $f(x, y)$*

Chapter 4
Algebraic constructs

Before we define the different number systems, like the natural numbers, whole numbers, rational numbers, real numbers and complex numbers, we define the algebraic operations and structures that we can define on them. In this way we abstract away the algebraic operations and algebraic structures. First we define the concept of a operator which is short notation for the application of a function with two arguments between a set and itself.

Definition 4.1. (Operator) *Let X be a set then a **operator** is function*

$$f: X \times X \rightarrow X$$

To avoid using excessive notation we use infix notation instead of the classic function call notation, so

$$f(x, y) \text{ is noted as } x f y$$

4.1 Groups

Definition 4.2. *A semi-group is a pair $\langle G, \odot \rangle$ where G is a set and $\odot$ a operator $\odot: G \times G \rightarrow G$ such that:*

neutral element. *$\exists e \in G$ such that $\forall x \in G$ we have $x \odot e = x = e \odot x$*

associativity. *$\forall x, y, z \in G$ we have $(x \odot y) \odot z = x \odot (y \odot z)$*

Theorem 4.3. *If $\langle G, \odot \rangle$ is a semi-group then*

1. *$G \neq \varnothing$*
2. *G has only one neutral element*

Proof.

1. As G is a group there exist a neutral element $e \in G$ so that $G \neq \varnothing$
2. Assume that there exists two neutral elements e, e' then we have

$$e \underset{e' \text{ is neutral element}}{=} e \odot e' \underset{e \text{ is neutral element}}{=} e' \qquad \square$$

Example 4.4. Let X be a set then $\langle X^X, \circ \rangle$ is a semi group [see definition: 2.25]. Here X^X is the set of function graphs between X and X and $\circ$ is the composition between functions.

Proof. As X is a set we have by [theorem: 2.30] that X^X is a set. Further if $f, g \in X^X$ then f: $X \rightarrow$ and $g: X \rightarrow X$ are functions, so that by [theorem: 2.45] $f \circ g: X \rightarrow X$ is a function, hence $f \circ g \in X^X$. So

$$\circ: X^X \times X^X \rightarrow X^X \text{ defined by } \circ(f, g) = f \circ g$$

is a function. The neutral element is Id_X because $\forall f \in X^X$ we have

$$f \circ \mathrm{Id}_X \underset{[\text{theorem: } 2.43}{=} f \underset{[\text{theorem: } 2.43}{=} \mathrm{Id}_X \circ f$$

$\square$

A group is a semi-group with the extra condition that is has a inverse element.

Definition 4.5. *A* ***group*** $\langle X, \odot \rangle$ *is a semi-group with the extra condition*

Inverse Element. $\forall x \in G$ *there* $\exists y \in G$ *such that*

$$x \odot y = e = y \odot x$$

where e is the neutral element of the group.

Theorem 4.6. *If* $\langle G, \odot \rangle$ *is group then every element has a unique inverse element. So*

$$\forall x \in G \ \exists! y \in G \text{ such that } x \odot y = x = y \odot x$$

this unique element is noted as x^{-1}.

Proof. Let $x \in G$ and assume that y, y' are inverse elements for x then we have

$$x \odot y = e = y \odot x \text{ and } x \odot y' = e = y' \odot x$$

So that

$$y = y \odot e = y \circ (x \odot y') = (y \odot x) \odot y' = e \odot y' = y'$$

□

Theorem 4.7. *If* $\langle G, \odot \rangle$ *is a group then* $\forall x, y \in G$ *we have* $(x \odot y)^{-1} = y^{-1} \odot x^{-1}$

Proof. We have

$$\begin{aligned}
(x \odot y) \odot (y^{-1} \odot x^{-1}) &= x \odot (y \odot (y^{-1} \odot x^{-1})) \\
&= x \odot ((y \odot y^{-1}) \odot x^{-1}) \\
&= x \odot (e \odot x^{-1}) \\
&= x \odot x^{-1} \\
&= e \\
(y^{-1} \odot x^{-1}) \odot (x \odot y) &= y^{-1} \odot (x^{-1} \odot (x \odot y)) \\
&= y^{-1} \odot ((x^{-1} \odot x) \odot y) \\
&= y^{-1} \odot (e \odot y) \\
&= y^{-1} \odot y \\
&= e
\end{aligned}$$

□

Theorem 4.8. *If* $\langle G, \odot \rangle$ *is a group then* $\forall x \in G$ *we have* $(x^{-1})^{-1} = x$ *and* $e^{-1} = e$ *where e is the neutral element.*

Proof. If $x \in G$ then $x \odot x^{-1} = e = x^{-1} \odot x$ and $(x^{-1})^{-1} \odot x^{-1} = e = x^{-1} \odot (x^{-1})^{-1}$. So

$$\begin{aligned}
x &= x \odot e \\
&= x \odot (x^{-1} \odot (x^{-1})^{-1}) \\
&= (x \odot x^{-1}) \odot (x^{-1})^{-1} \\
&= e \circ (x^{-1})^{-1} \\
&= (x^{-1})^{-1}
\end{aligned}$$

Further

$$e^{-1} = e \cdot e^{-1} = e$$

□

Theorem 4.9. *If* $\langle G, \odot \rangle$ *then* $\forall x, y \in X$ *we have* $x = y \Leftrightarrow x^{-1} = y^{-1}$

Proof.

⇒. $e = x^{-1} \cdot x = x^{-1} \cdot y$ and $e = x \cdot x^{-1} = y \cdot x^{-1}$ proving by uniqueness of the inverse [see theorem: 4.6] that $y^{-1} = x^{-1}$

$\Leftarrow$. If $x^{-1}=y^{-1}$ then by the above we have $(x^{-1})^{-1}=(y^{-1})^{-1}$ it follows from [theorem: 4.8] that $x=y$.

□

Definition 4.10. *A semi-group or group $\langle G,\odot\rangle$ is abelian or **commutative** iff*

$$\forall x,y\in G \text{ we have } x\odot y=y\odot x$$

Definition 4.11. *Let $\langle G,\odot\rangle$ be a semi-group then $F\subseteq G$ is a sub-semi-group iff*

1. *$\forall x,y\in F$ we have $x\odot y\in F$*
2. *$e\in F$ [e is the neutral element of G]*

Definition 4.12. *Let $\langle G,\odot\rangle$ be groups then $F\subseteq G$ is a sub-group iff*

1. *$\forall x,y\in F$ we have $x\odot y\in F$*
2. *$e\in F$ [e is the neutral element of G]*
3. *$\forall x\in F$ we have $x^{-1}\in F$*

The following show how sub-semi-groups and sub-groups can be used to reduce the work for proving the group axioms.

Theorem 4.13. *Let $\langle G,\odot\rangle$ be a semi-group and $F\subseteq G$ a sub-semi-group then*

1. *$\langle F,\odot_{|F\times F}\rangle$ is a semi group*
2. *If $\langle G,\odot\rangle$ is abelian then $\langle F,\odot_{|F\times F}\rangle$ is abelian*

To avoid excessive notation we use $\odot$ instead of $\odot_{|F\times F}$ if it is clear from the context which operation should be used.

Proof. First as G is a set we have by the Axiom of Subsets [axiom: 1.54] that G is a set.

1. For $\langle F,\odot_{|F\times F}\rangle$

   neutral element. By definition of a subgroup $e\in F$. Let $x\in F$ then

   $$e\odot_{|F\times F}x\underset{e,x\in F}{=}e\odot x=x=x\odot e=x\odot_{|F\times F}e$$

   associativity. Let $x,y,z\in F$ then

   $$(x\odot_{|F\times F}y)\odot_{|F\times F}z=(x\circ y)\circ z=x\circ(y\circ z)=x\odot_{|F\times F}(y\odot_{|F\times F}z)$$

2. Let $x,y\in F$ then

   $$x\odot_{|F\times F}y=x\odot y=y\odot x=y\odot_{|F\times F}x$$

□

Theorem 4.14. *Let $\langle G,\odot\rangle$ be a group and $F\subseteq G$ a sub-group then*

1. *$\langle F,\odot_{|F\times F}\rangle$ is a group*
2. *If $\langle G,\odot\rangle$ is abelian then $\langle F,\odot_{|F\times F}\rangle$ is abelian*

To avoid excessive notation we use $\odot$ instead of $\odot_{|F\times F}$ if it is clear from the context which operation should be used.

Proof.

1. For $\langle F,\odot_{|F\times F}\rangle$ we have

   neutral element. Let $x\in F$ then $e\odot_{|F\times F}x\underset{e,x\in F}{=}e\odot x=x=x\odot e=x\circ_{,|F\times F}e$

   associativity. Let $x,y,z\in F$ then

   $$(x\odot_{|F\times F}y)\odot_{|F\times F}z=(x\circ y)\circ z=x\circ(y\circ z)=x\odot_{|F\times F}(y\odot_{|F\times F}z)$$

inverse element. Let $x \in F$ then also $x^{-1} \in F$ then

$$(x \odot_{|F \times F} x^{-1}) = x \odot x^{-1} = e = x^{-1} \odot c = x^{-1} \odot_{|F \times F} x$$

2. Let $x, y \in F$ then

$$x \odot_{|F \times F} y = x \odot y = y \odot x = y \odot_{|F \times F} x$$ □

Example 4.15. Let X be a set, $\langle X^X, \circ \rangle$ the semi-group from [example: 4.4] then $\langle \mathcal{B}[X], \circ \rangle$ is a group where $\mathcal{B}[X] = \{f \in X^X | f: X \to X \text{ is a bijection}\}$.

Proof. First we prove that $\mathcal{B}[X]$ is a sub-semi-group

1. $\forall f, g \in \mathcal{B}[X]$ we have that $f: X \to X$ and $g: X \to X$ are bijections so that by [theorem: 2.69] $f \circ g$ is a bijection so that $f \circ g \in \mathcal{B}[X]$
2. $\mathrm{Id}_X: X \to X$ is by [theorem: 2.60] a bijection so that $\mathrm{Id}_X \in \mathcal{B}[X]$

Applying then [theorem: 4.13] proves that

$$\langle \mathcal{B}[X], \circ \rangle \text{ is a semi-group}$$

Let $f \in \mathcal{B}[X]$ then $f: X \to X$ is a bijection and by [theorems: 2.64,2.67] we have that $f^{-1}: X \to X$ is a bijection, so that $f^{-1} \in \mathcal{B}[X]$ and $f \circ \mathrm{Id}_X = f = \mathrm{Id}_X \circ f$. □

Definition 4.16. (Group Homeomorphism) *If $\langle F, \odot \rangle$ and $\langle G, \oplus \rangle$ be semi-groups then a function $f: F \to G$ is a **group homeomorphism** if $\forall x, y \in F$ we have $f(x \odot y) = f(x) \oplus g(y)$.*

Theorem 4.17. *If $\langle F, \odot \rangle$ and $\langle G, \oplus \rangle$ be groups with neutral elements e_F, e_G and $f: F \to G$ a **group homeomorphism** then:*

1. *$f(e_F) = e_G$*
2. *$\forall x \in F$ we have $f(x^{-1}) = f(x)^{-1}$*

Proof.

1.

$$\begin{aligned} e_G &= f(e_F)^{-1} \oplus f(e_F) \\ &= f(e_F)^{-1} \oplus f(e_F \odot e_F) \\ &= f(e_F)^{-1} \oplus (f(e_F) \oplus f(e_F)) \\ &= (f(e_F)^{-1} \oplus f(e_F)) \oplus f(e_F) \\ &= e_G \circ f(e_F) \\ &= f(e_F) \end{aligned}$$

2. If $x \in F$ then

$$f(x^{-1}) \oplus f(x) = f(x^{-1} \odot x) = f(e_F) \underset{(1)}{=} e_G$$

and

$$f(x) \oplus f(x^{-1}) = f(x \odot x^{-1}) = f(e_F) \underset{(1)}{=} e_G$$

so that $f(x)^{-1} = f(x^{-1})$ □

Definition 4.18. (Group Isomorphism) *If $\langle F, \odot \rangle$ and $\langle G, \oplus \rangle$ are semi-groups then a **group isomorphism** is a **bijection** $f: F \to G$ that is a **group homeomorphism**.*

Theorem 4.19. *Let $\langle F, \odot \rangle$, $\langle G, \oplus \rangle$ be semi groups and*

$$f: F \to G$$

is a group isomorphism then

$$f^{-1}: G \to F$$

is a group isomorphism.

Proof. As $f: F \rightarrow G$ is a bijection we have by [theorem: 2.67] that $f^{-1}: G \rightarrow F$ is a bijection. Take $x, y \in G$ then we have

$$\begin{array}{rcl} f^{-1}(x \oplus y) & = & f^{-1}(\mathrm{Id}_G(x) \oplus \mathrm{Id}_G(y)) \\ & \underset{\text{[theorem: 2.64}}{=} & f^{-1}((f \circ f^{-1})(x) \oplus (f \circ f^{-1})(y)) \\ & \underset{\text{[theorem: 2.37]}}{=} & f^{-1}(f(f^{-1}(x)) \oplus f(f^{-1}(y))) \\ & \underset{f \text{ is homeomorphism}}{=} & f^{-1}(f(f^{-1}(x) \odot f^{-1}(y))) \\ & \underset{\text{[theorem: 2.37]}}{=} & (f^{-1} \circ f)(f^{-1}(x) \odot f^{-1}(y)) \\ & \underset{\text{[theorem: 2.64}}{=} & \mathrm{Id}_F(f^{-1}(x) \odot f^{-1}(y)) \\ & = & f^{-1}(x) \odot f^{-1}(y) \end{array}$$

Further if e_F, e_G are the neutral elements of $\langle F, \oplus_F \rangle$, $\langle G, \oplus_G \rangle$ then

$$\begin{array}{rcl} e_F & = & \mathrm{Id}_F(e_f) \\ & = & (f^{-1} \circ f)(e_F) \\ & = & f^{-1}(f(e_F)) \\ & = & f^{-1}(e_G) \end{array}$$

proving that

$$f^{-1}: F \rightarrow G \text{ is a group isomorphism}$$ □

The following theorem show how we can define a group on the product of a family of groups.

Theorem 4.20. *Let $\{\langle A_i, \odot_i \rangle\}_{i \in I}$ be a family of semi-groups then we have*

1. *If $x, y \in \prod_{i \in I} A_i$ then $(x \odot y) \in \prod_{i \in I} A_i$ where $x \odot y$ is defined by $(x \odot y)_i = x_i \odot_i y_i$*
2. *If we define $\odot: (\prod_{i \in I} A_i) \times (\prod_{i \in I} A_i) \rightarrow \prod_{i \in I} A_i$ by $\odot(x, y) = x \odot y$ then*

$$\left\langle \prod_{i \in I} A_i, \odot \right\rangle$$

   is a semi-group with neutral element e defined by $(e)_i = e_i$ where e_i is the neutral element of $\langle A_i, \odot_i \rangle$
3. *If $\forall i \in I$ we have that $\langle A_i, \odot_i \rangle$ is abelian then $\langle \prod_{i \in I} A_i, \odot \rangle$ is abelian.*
4. *If $\forall i \in I$ we have that $\langle A_i, \odot_i \rangle$ is a group then $\langle \prod_{i \in I} A_i, \odot \rangle$ is a group where the inverse x^{-1} for each $x \in \prod_{i \in I} A_i$ is defined by $(x^{-1})_i = (x_i)^{-1}$ [here $(x_i)^{-1}$ is the inverse of x_i in the group $\langle A_i, \odot_i \rangle$*

Proof.

1. If $x, y \in \prod_{i \in I} A_i$ then x is a function $x: I \rightarrow \bigcup_{i \in I} A_i$ such that $\forall i \in I$ $x_i = x(i) \in A_i$ and y is a function $y: I \rightarrow \bigcup_{i \in I} A_i$ such that $\forall i \in I$ $y_i = y(i) \in A_i$. So if we define $x \odot y$ by $(x \odot y)(i) = (x \odot y)_i = x_i \odot_i y_i = x(i) \odot_i y(i)$ then $x \odot y: I \rightarrow \bigcup_{i \in I} A_i$ is a function and $\forall i \in I$ we have $(x \odot y)(i) = x(i) \odot_i y(i) \in A_i$ [as $\langle A_i, \odot_i \rangle$ is a semi-group]. Hence $x \odot y \in \prod_{i \in I} A_i$
2. We have

   associativity. Let $x, y, z \in \prod_{i \in I} A_i$ then we have for $i \in I$

$$\begin{array}{rcl} (x \odot (y \odot z))(i) & = & x(i) \odot_i (y \odot z)(i) \\ & = & x(i) \odot_i (y(i) \odot_i z(i)) \\ & \underset{\langle A_i, \odot_i \rangle \text{ is a semi group}}{=} & (x(i) \odot y(i)) \odot z(i) \\ & = & (x \odot y)(i) \odot_i z(i) \\ & = & ((x \odot y) \odot z)(i) \end{array}$$

so that

$$x \odot (y \odot z) = (x \odot y) \odot z$$

neutral element. Let $x \in \prod_{i \in I} A_i$ then $\forall i \in I$

$$\begin{aligned}
(x \odot e)(i) &= x(i) \odot_i e(i) \\
&= x(i) \odot_i e_i \\
&\underset{\langle A_i, \odot_i \rangle \text{ is a semi group}}{=} x(i) \\
(e \odot x)(i) &= e(i) \odot_i x(i) \\
&= e_i \odot_i x(i) \\
&\underset{\langle A_i, \odot_i \rangle \text{ is a semi group}}{=} x(i)
\end{aligned}$$

so that

$$x \odot e = x = e \odot x$$

3. Let $x, y \in \prod_{i \in I} A_i$ then $\forall i \in I$ we have

$$(x \circ y)(i) = x(i) \odot_i y(i) \underset{\langle A_i, \odot_i \rangle \text{ is abelian}}{=} y(i) \odot_i x(i) = (y \odot x)(i)$$

so that $x \odot y = y \odot x$

4. Let $x \in \prod_{i \in I} A_i$ then we have $\forall i \in I$ that

$$\begin{aligned}
(x \odot x^{-1})(i) &= x(i) \odot_i (x^{-1})(i) \\
&= x(i) \odot_i (x_i)^{-1} \\
&= x_i \odot_i (x_i)^{-1} \\
&\underset{\langle A_i, \odot_i \rangle \text{ is a group}}{=} e_i \\
&= e(i) \\
(x^{-1} \odot x)(i) &= (x^{-1})(i) \odot_i x(i) \\
&= (x_i)^{-1} \odot_i x(i) \\
&= (x_i)^{-1} \odot_i x_i \\
&= e_i \\
&= e(i)
\end{aligned}$$

So that $x \odot x^{-1} = e = x^{-1} \odot x$. Which as by (2) $\langle \prod_{i \in I} A_i, \odot \rangle$ is a semi group proves that $\langle \prod_{i \in I} A_i, \odot \rangle$ is a group. $\square$

The following five definitions will be later used in Linear Algebra.

Definition 4.21. *Let $\langle G, \odot \rangle$ be a group with neutral element e and let X be a set then we have the following definitions:*

1. *A **left group action** is a function $\triangleright: G \times X \rightarrow X$ where $\triangleright(g, x) \underset{\text{notation}}{=} g \triangleright x$ such that*
   a. *$\forall x \in X$ we have $e \triangleright x = x$*
   b. *$\forall g, g' \in G$ and $\forall x \in X$ we have $(g \odot g') \triangleright x = g \triangleright (g' \triangleright x)$*
2. *A **right group action** is a function $\triangleleft: X \times G \rightarrow X$ where $\triangleleft(x, g) \underset{\text{notation}}{=} x \triangleleft g$ such that*
   a. *$\forall x \in X$ we have $x \triangleleft e = x$*
   b. *$\forall g, g' \in G$ and $\forall x \in X$ we have $x \triangleleft (g \odot g') = (x \triangleleft g) \triangleleft g'$*

Definition 4.22. *Let $\langle G, \odot \rangle$ be a group, X a set, $\triangleright$ a left group action and $g \in G$ then we define*

$$g_{\triangleright}: X \rightarrow X \text{ by } g_{\triangleright}(x) = g \triangleright x$$

Definition 4.23. *Let $\langle G, \odot \rangle$ be a group, X, $\triangleleft$ a right group action and $g \in G$ then we define*

$$g_{\triangleleft}: X \rightarrow X \text{ by } g_{\triangleleft}(x) = x \triangleleft g$$

Definition 4.24. *Let $\langle G, \odot \rangle$ be a group with neutral element e and let X be a set then we have the following definitions for a left group action $\triangleright$*

1. *$\triangleright$ is **faithful** if*

$$g_{\triangleright} = \mathrm{Id}_X \text{ if and only if } g = e$$

or equivalently

$$\{g \in G | \forall x \in X \text{ we have } g \triangleright x = x\} = \{e\}$$

2. *$\triangleright$ is **transitive** iff $\forall x_1, x_2$ there exist a $g \in G$ such that $g \triangleright x_1 = x_2$*
3. *$\triangleright$ is **free** iff $\forall x \in X$ we have $\{g \in G | g \triangleright x = x\} = \{e\}$*

Definition 4.25. *Let $\langle G, \odot \rangle$ be a group with neutral element e and let X be a set then we have the following definitions for a right group action $\triangleleft$*

1. *$\triangleright$ is **faithful** if*

$$g_{\triangleleft} = \mathrm{Id}_X \text{ if and only if } g = e$$

or equivalently

$$\{g \in G | \forall x \in X \text{ we have } g \triangleleft x = x\} = \{e\}$$

2. *$\triangleright$ is **transitive** iff $\forall x_1, x_2$ there exists a $g \in G$ such that $g \triangleleft x_1 = x_2$*
3. *$\triangleright$ is **free** iff $\forall x \in X$ we have $\{g \in G | g \triangleleft x = x\} = \{e\}$*

4.2 Rings

Definition 4.26. (Ring) *A triple $\langle R, \oplus, \odot \rangle$ is a ring iff*

1. *R is a set*
2. *$\langle R, \oplus \rangle$ is a abelian group or $\oplus: R \times R \to R$ is a operator such that*

   associativity. *$\forall x, y, z \in R$ we have $x \oplus (y \oplus z) = (x \oplus y) \oplus z$*

   neutral element. *$\exists 0 \in R$ such that $\forall x \in R$ we have $0 \oplus x = x = x \oplus 0$*

   inverse element. *$\forall x \in R$ there exist a $-x$ such that $x \oplus (-x) = 0 = (-x) \oplus x$*

   commutativity. *$\forall x, y \in R$ we have $x \oplus y = y \oplus x$*

   $\oplus$ is called the sum operator of the ring.
3. *$\odot: R \times R \to R$ is a operator so that*

   distributivity. *$\forall x, y, z \in R$ we have $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$*

   neutral element. *$\exists 1 \in R$ such that $\forall x \in R$ we have $1 \odot x = x = x \odot 1$*

   commutativity. *$\forall x, y \in R$ we have $x \odot y = y \odot x$*

   associativity. *$\forall x, y, z \in R$ we have $x \odot (y \odot z) = (x \odot y) \odot z$*

   $\odot$ is called the multiplication operator of the ring.

Definition 4.27. *If $\langle R, \oplus, \odot \rangle$ is a ring then a **zero divisor of R** is a $x \in R \setminus \{0\}$ so that $\exists y \in R \setminus \{0\}$ such that $x \odot y = 0$*

Definition 4.28. *A ring $\langle R, \oplus, \odot \rangle$ is a **integral domain** if it does not contains a **zero divisor***

Definition 4.29. (Subring) *If $\langle R, \oplus, \odot \rangle$ is a ring then a subset $S \subseteq R$ is a subring iff*

1. *$\forall x, y \in S$ we have $x \oplus y \in S$ and $x \odot y \in S$*
2. *$\forall x \in S$ we have $-x \in S$ [the inverse element for $\oplus$]*
3. *$1 \in S$ [the neutral element for $\odot$]*
4. *$0 \in S$ [the neutral element for $\oplus$]*

Theorem 4.30. *If $\langle R, \oplus, \odot\rangle$ is a ring and $S \subseteq R$ a subring then $\langle S, \oplus_{|S\times S}, \odot_{|S\times S|}\rangle$ is a ring. For simplicity we note this ring as $\langle S, \oplus, \odot\rangle$*

Proof.

1. S is a set as R is a set by the Axiom of Subsets [axiom: 1.54].
2. $\langle S, \oplus_{|S\times S}\rangle$ is a abelian group by [theorem: 4.13]
3. $\odot: R\times R \to R$ is a operator so that

   Distributivity. $\forall x, y, z \in S$ we have

   $$x \odot_{|S\times S} (y \oplus_{|S\times S} z) = x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z) = (x \odot_{|S\times S} y) \oplus_{|S\times S} (x \odot_{|S\times S} z)$$

   neutral element. For $1 \in R$ we have $\forall x \in S$ that

   $$1 \odot_{|S\times S} x = 1 \odot x = x = x \odot 1 = x \odot_{|S\times S} 1$$

   commutativity. $\forall x, y \in S$ we have

   $$x \odot_{|S\times S} y = x \odot y = y \odot x = y \odot_{|S\times S} x$$

   associativity. $\forall x, y, z \in S$ we have

   $$x \odot_{|S\times S} (y \odot_{|S\times S} z) = x \odot (y \odot z) = (x \odot y) \odot z = (x \odot_{|S\times S} y) \odot_{|S\times S} z$$ □

The following theorem shows that the neutral element for the sum in a ring is actual a absorbing element.

Theorem 4.31. *Let $\langle X, \oplus, \odot\rangle$ be a ring with 0 the neutral element for $\oplus$ then $\forall x \in R$ we have*

$$x \odot 0 = 0 = 0 \odot x$$

Proof. If $x \in R$ then

$$\begin{aligned} 0 &\underset{\text{inverse element}}{=} (0 \odot x) \oplus -(0 \odot x) \\ &\underset{0\oplus 0=0}{=} ((0 \oplus 0) \odot x) \oplus (-(0 \odot x)) \\ &\underset{\text{distributivity}}{=} [(0 \odot x) \oplus (0 \odot x)] \oplus (-(0 \odot x)) \\ &\underset{\text{associativity}}{=} (0 \odot x) \oplus [(0 \odot x) + (-(0 \odot x))] \\ &\underset{\text{inverse element}}{=} (0 \odot x) \oplus 0 \\ &\underset{\text{inverse element}}{=} 0 \odot x \\ &\underset{\text{commutativity}}{=} x \odot 0 \end{aligned}$$

□

Definition 4.32. *Let $\langle A, \oplus_A, \odot_A\rangle$ and $\langle B, \oplus_B, \odot_B\rangle$ be rings then a function $f: A \to B$ is is a* ***ring homeomorphism*** *iff*

1. *$\forall x, y \in A$ we have $f(x \oplus_A y) = f(x) \oplus_B f(y)$*
2. *$\forall x, y \in A$ we have $f(x \odot_A y) = f(x) \odot_B f(y)$*
3. *$f(1_A) = 1_B$ where 1_A is the multiplicative neutral element in A and 1_B is the multiplicative neutral element in B.*

Note that a ring homeomorphism $f: A \to B$ for the rings $\langle A, \oplus_A, \odot_A\rangle, \langle B, \oplus_B, \odot_B\rangle$ is automatically a group homeomorphism for the groups $\langle A, \oplus_A\rangle, \langle B, \oplus_B\rangle$. Using 4.17 we have then the following theorem

Theorem 4.33. *If $\langle A, \oplus_A, \odot_A\rangle$ and $\langle B, \oplus_B, \odot_B\rangle$ are rings with additive units $0_A, 0_B$ and $f: A \to B$ a ring homeomorphism then we have*

1. *$f(0_A) = 0_B$*

2. $\forall a \in A$ *we have* $f(-a) = -f(a)$

Definition 4.34. *If* $\langle A, \oplus_A, \odot_A\rangle$ *and* $\langle B, \oplus_B, \odot_B\rangle$ *are rings then a function* $f: A \rightarrow B$ *is a ring homeomorphism if it is a ring homeomorphism and a bijection.*

4.3 Fields

A ring has no inverse for a multiplicative element, one of the reasons for this is that is is difficult to say what the inverse of 0 is, as expressed in the following computation

$$1 = 0 \odot 0^{-1} \underset{[\text{theorem: } 4.31]}{=} 0$$

so that we have

$$\forall x \in R \text{ that } x = 1 \odot x = 0 \odot x \underset{[\text{theorem: } 4.31]}{=} 0$$

and we end up with $R = \{0\}$, which is not a useful ring. However we can avoid this problem if we exclude the 0 of the list of elements that has a inverse element. This is the idea behind a field.

Definition 4.35. *A triple* $\langle F . \oplus, \odot\rangle$ *is a field if* $\langle F, \oplus, \odot\rangle$ *is a ring and additional*

$$\forall x \in F \setminus \{0\}\ \exists b \in F \text{ such that } x \odot b = 1 = b \odot x$$

where 1 *is the neutral element for* $\odot$. *In other words* $\langle F, \oplus, \odot\rangle$ *is a field iff*

1. F *is a set*
2. $\langle F, \oplus\rangle$ *is a abelian group or* $\oplus: F \times F \rightarrow F$ *is a operator such that*

   associativity. $\forall x, y, z \in F$ *we have* $x \oplus (y \oplus z) = (x \oplus y) \oplus z$

   neutral element. $\exists 0 \in F$ *such that* $\forall x \in F$ *we have* $0 \oplus x = x = x \oplus 0$

   inverse element. $\forall x \in F$ *there exist a* $-x$ *such that* $x \oplus (-x) = 0 = (-x) \oplus x$

   commutativity. $\forall x, y \in F$ *we have* $x \oplus y = y \oplus x$

   $\oplus$ *is called the sum operator of the field.*
3. $\odot: F \times F \rightarrow F$ *is a operator so that*

   Distributivity. $\forall x, y, z \in F$ *we have* $x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$

   neutral element. $\exists 1 \in F$ *such that* $\forall x \in F$ *we have* $1 \odot x = x = x \odot 1$

   commutativity. $\forall x, y \in F$ *we have* $x \odot y = y \odot x$

   associativity. $\forall x, y, z \in F$ *we have* $x \odot (y \odot z) = (x \odot y) \odot z$

   inverse element. $\forall x \in F \setminus \{0\}\ \exists b \in F$ *such that* $x \odot b = 1 = b \odot x$

   $\odot$ *is called the multiplication operator of the field.*

The inverse if it exist is unique

Theorem 4.36. *If* $\langle F, \oplus, \odot\rangle$ *then* $\forall x \in F \setminus \{0\}$ *there exist a* ***unique*** *inverse element for* $\odot$. *We note this element as* x^{-1}.

Proof. Let $x \in F \setminus \{0\}$ and assume that $y, y' \in F$ such that $y \odot x = 1 = x \odot y$ and $y' \odot x = 1 = x \odot y'$ then we have

$$y = y \odot 1 = y \circ (x \odot y') = (y \odot x) \odot y' = 1 \odot y' = y' \qquad \square$$

Definition 4.37. *If* $\langle F, \oplus, \odot\rangle$ *is a field then a subset* $S \subseteq F$ *is a subfield iff the following is satisfied*

1. $\forall x, y \in F$ *we have* $x \oplus y \in F$ *and* $x \odot y \in F$
2. $\forall x \in F$ *we have* $-x \in F$ *[the inverse element for* $\oplus$*]*

3. $1 \in F$ *[the neutral element for* $\odot$*]*
4. $0 \in F$ *[the neutral element for* $\oplus$*]*
5. $\forall x \in F \setminus \{0\}$ *we have* $x^{-1} \in F$

Theorem 4.38. *If* $\langle F, \oplus, \odot \rangle$ *is a field and* $S \subseteq F$ *is a subfield then* $\langle S, \oplus_{|S \times S}, \odot_{|S \times S} \rangle$ *is a field*

Proof. Using [theorem: 4.30] it follows that $\langle S, \oplus_{|S \times S}, \odot_{|S \times S} \rangle$ is a ring. Further if $x \in F \setminus \{0\}$ then $1 \in S$ and $x^{-1} \in S$, further $x \odot_{|S} x^{-1} = x \odot x^{-1} = 1 = x^{-1} \odot x = x^{-1} \odot_{|S} x$ proving that $\langle S, \oplus_{|S \times S}, \odot_{|S \times S} \rangle$ is a field. □

Definition 4.39. *If* $\langle A, \odot_A, \oplus_A \rangle$ *and* $\langle B, \odot_B, \oplus_B \rangle$ *are fields with multiplicative units* $1_A, 1_B$ *then a function* $f: A \rightarrow B$ *is a field homeomorphism iff*

1. $\forall x, y \in A$ *we have* $f(x \odot_A y) = f(x) \odot_B f(y)$
2. $\forall x, y \in A$ *we have* $f(x \oplus_A y) = f(x) \oplus_B f(y)$
3. $f(1_A) = 1_B$

If f *is also a bijection then we call* f *a* ***field isomorphism****.*

Note that a field homeomorphism $f: A \rightarrow B$ is automatically a group homeomorphism.

Theorem 4.40. *If* $\langle A, \odot_A, \oplus_A \rangle$ *and* $\langle B, \odot_B, \oplus_B \rangle$ *are fields with multiplicative units* $1_A, 1_B$ *and*

$$f: A \rightarrow B$$

is a field isomorphism then $f^{-1}: B \rightarrow A$ *is a field isomorphism*

Proof. First using [theorem: 2.67] we have that $f^{-1}: B \rightarrow A$ is a bijection. Further we have:

1. Take $x, y \in B$ then we have

$$\begin{array}{rcl} f^{-1}(x \oplus_B y) & = & f^{-1}(\mathrm{Id}_B(x) \oplus_B \mathrm{Id}_B(y)) \\ & \underset{\text{[theorem: 2.64]}}{=} & f^{-1}((f \circ f^{-1})(x) \oplus_B (f \circ f^{-1})(y)) \\ & \underset{\text{[theorem: 2.37]}}{=} & f^{-1}(f(f^{-1}(x)) \oplus_B f(f^{-1}(y))) \\ & \underset{f \text{ is homeomorphism}}{=} & f^{-1}(f(f^{-1}(x) \oplus_A f^{-1}(y))) \\ & \underset{\text{[theorem: 2.37]}}{=} & (f^{-1} \circ f)(f^{-1}(x) \oplus_A f^{-1}(y)) \\ & \underset{\text{[theorem: 2.64]}}{=} & \mathrm{Id}_A(f^{-1}(x) \oplus_A f^{-1}(y)) \\ & = & f^{-1}(x) \oplus_A f^{-1}(y) \end{array}$$

2. Take $x, y \in B$ then we have

$$\begin{array}{rcl} f^{-1}(x \odot_B y) & = & f^{-1}(\mathrm{Id}_B(x) \odot_B \mathrm{Id}_B(y)) \\ & \underset{\text{[theorem: 2.64]}}{=} & f^{-1}((f \circ f^{-1})(x) \odot_B (f \circ f^{-1})(y)) \\ & \underset{\text{[theorem: 2.37]}}{=} & f^{-1}(f(f^{-1}(x)) \odot_B f(f^{-1}(y))) \\ & \underset{f \text{ is homeomorphism}}{=} & f^{-1}(f(f^{-1}(x) \odot_A f^{-1}(y))) \\ & \underset{\text{[theorem: 2.37]}}{=} & (f^{-1} \circ f)(f^{-1}(x) \odot_A f^{-1}(y)) \\ & \underset{\text{[theorem: 2.64]}}{=} & \mathrm{Id}_A(f^{-1}(x) \odot_A f^{-1}(y)) \\ & = & f^{-1}(x) \odot f^{-1}(y) \end{array}$$

3. From $f(1_A) = 1_B$ it follows that

$$f^{-1}(1_B) = f^{-1}(f(1_B)) = (f^{-1} \circ f)(1_B) \underset{\text{[theorem: 2.64]}}{=} \mathrm{Id}_A(1_B) = 1_B$$

□

Theorem 4.41. *If* $\langle A, \oplus_A, \odot_A\rangle$ *and* $\langle B, \oplus_B, \odot_B\rangle$ *are fields with additive units* $0_A, 0_B$ *and multiplicative units* 1_A,1_B *and* $f: A \rightarrow B$ *a field homeomorphism then we have*

1. $f(0_A) = 0_B$
2. $\forall a \in A$ *we have* $f(-a) = -f(a)$
3. $\forall a \in A$ *with* $a \neq 0_A$ *we have* $f(a^{-1}) = (f(a))^{-1}$

Proof. As field homeomorphism $f: A \rightarrow B$ for the fields $\langle A, \oplus_A, \odot_A\rangle, \langle B, \oplus_B, \odot_B\rangle$ is automatically a group homeomorphism for the groups $\langle A, \oplus_A\rangle, \langle B, \oplus_B\rangle$ we have by 4.17 that (1) and (2) are valid. As for (3), if $x \in A$ with $x \neq 0_A$ then there exists a x^{-1} such that $x^{-1} \cdot x = 1_A$ hence

$$1_B = f(1_A) = f(x^{-1} \odot_A x) = f(x^{-1}) \odot_B f(x) \underset{\text{commutativity}}{=} f(x) \odot_B f(x^{-1})$$

proving by [theorem: 4.36] that $f(x^{-1}) = (f(x))^{-1}$. $\square$

Chapter 5
Natural Numbers

5.1 Definition of the Natural Numbers

We are now ready to define the first set of numbers namely the natural numbers which forms the basic of the other number systems but also of the important concepts of finite, infinite sets, countable sets, recursion and mathematical induction. To define the set of natural numbers recall the following definitions and axiom.

Definition 5.1. (Successor Set) *A **set** A is a **successor set** iff*

1. $\varnothing \in A$
2. *If* $X \in A \Rightarrow X \bigcup \{X\} \in A$

[see definition: 1.51]

Axiom 5.2. (Axiom of Infinity) *There exists a successor set [see axiom: 1.52].*

Definition 5.3. (Natural numbers) *The set of **natural numbers** $\mathbb{N}_0$ **is defined** by*

$$\mathbb{N}_0 = \bigcap \{S | S \textit{ is a successor set}\}$$

Theorem 5.4. $\mathbb{N}_0$ *is a set*

Proof. By the axiom of infinity it follows that $\{S | S \text{ is a successor set}\} \neq \varnothing$ so that by [theorem: 1.60 (5)] $\bigcap \{S | S \text{ is a successor set}\}$ is a set. $\square$

Theorem 5.5. *If* $n \in \mathbb{N}_0$ *then* $n \bigcup \{n\} \in \mathbb{N}_0$

Proof. If $n \in \mathbb{N}_0$ then for $\forall A \in \{S | S \text{ is a successor set}\}$ we have $n \in A$ so that by definition of a successor set we have $n \bigcup \{n\} \in A$ so that $n \bigcup \{n\} \in \bigcap \{S | S \text{ is a successor set}\} = \mathbb{N}_0$. $\square$

The above theorem allows us to define the successor function

Definition 5.6. (Successor Function) *The function defined by*

$$s: \mathbb{N}_0 \to \mathbb{N}_0 \textit{ where } s(n) = n \bigcup \{n\}$$

*is called the **successor function**.*

The set $\mathbb{N}_0$ is not empty as is shown in the next theorem.

Theorem 5.7. $\varnothing \in \mathbb{N}_0$

Proof. If A is a successor set then by definition $\varnothing \in A$ so that $\varnothing \in \bigcap \{A | A \text{ is a successor set}\}$ $\square$

Further using the successor function we have that $s(\varnothing)$, $s(s(\varnothing))$ etc. are all elements of $\mathbb{N}_0$,. we introduce a special notation for this elements that corespondents with the notation used for counting.

Notation 5.8. *We define the numbers 0,1,2,3,... as follows*

1. $0 = \varnothing$
2. $1 = s(0) = s(\varnothing) = \varnothing \bigcup \{\varnothing\} = \{\varnothing\} = \{0\}$
3. $2 = s(1) = s(\varnothing) \bigcup \{s(\varnothing)\} = \{\varnothing\} \bigcup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} = \{0, 1\}$
4. $3 = s(2) = \{\varnothing, \{\varnothing\}\} \bigcup \{\{\varnothing, \{\varnothing\}\}\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} = \{0, 1, 2\}$
5. ...

The notation $\mathbb{N}_0$ may seem a little bit strange, the fact is that many mathematicians don't consider 0 a natural number. To express that $0 \in \mathbb{N}_0$ we add the 0 subscript. If we want to indicate that $0 \notin \mathbb{N}_0$ we use the following definition.

Definition 5.9. $\mathbb{N} = \mathbb{N}_0 \setminus \{0\}$

Theorem 5.10. *If $n \in \mathbb{N}_0$ then $s(n) \neq 0$*

Proof. By definition we have $s(n) = n \bigcup \{n\}$ so that $n \in s(n)$ proving that $s(n) \neq \varnothing = 0$ □

We introduce now the very important principle of **Mathematical Induction**.

Theorem 5.11. (Mathematical Induction) *If $X \subseteq \mathbb{N}_0$ such that*

1. $0 \in X$
2. *If $n \in X$ then $s(n) \in X$*

then $X = \mathbb{N}_0$

Proof. By $(1), (2)$ it follows that X is a successor set so that $X \in \{A | A \text{ is a successor set}\}$ hence by [theorem: 1.60] $\mathbb{N}_0 = \bigcap \{A | A \text{ is a successor set}\} \subseteq X$, which together with $X \subseteq \mathbb{N}$ proves that $X = \mathbb{N}$. □

Theorem 5.12. *Let $n, m \in \mathbb{N}_0$ then if $m \in s(n)$ we have $m \in n \vee m = n$*

Proof. If $m \in s(n) = n \bigcup \{n\}$ then we have either $m \in n$ or $m \in \{n\} \Rightarrow m = n$ □

Definition 5.13. *A set A is **transitive** if $\forall x \in A$ we have $x \subseteq A$.*

As a application of mathematical induction we prove that every natural number is transitive, this fact will be used later, when we define a order relation on $\mathbb{N}_0$ to prove transitivity, hence the name for this property.

Theorem 5.14. *$\forall n \in \mathbb{N}_0$ we have that n is transitive [in other words $\forall x \in n$ we have $x \subseteq n$]*

Proof. We prove this by mathematical induction, let $\mathcal{S} = \{n \in \mathbb{N}_0 | n \text{ is transitive}\}$ then clearly $S \subseteq \mathbb{N}_0$. Further we have

$0 \in S$. Because $\forall x \in \emptyset \vdash x \subseteq \emptyset$ is satisfied vacuously.

$n \in S \Rightarrow s(n) \in S$. If $n \in S$ then we have for $m \in s(n)$ by the previous theorem [theorem: 5.12] the following cases:

$m \in n$. Then as $n \in S$, n is transitive so that $m \subseteq n \subseteq n \bigcup \{n\} = s(n)$

$m = n$. Then $m = n \subseteq n \bigcup \{n\} = s(n)$

So $\forall m \in s(n)$ we have $m \subseteq s(n)$ which proves that $s(n)$ is transitive, hence $s(n) \in S$

Using mathematical induction [see theorem: 5.11] it follows then that $S = \mathbb{N}_0$. So if $n \in \mathbb{N}_0$ then $n \in S$ or n is transitive. □

Another application of transitivity and mathematical induction is the following theorem.

Theorem 5.15. *If* $n \in \mathbb{N}_0$ *then* $n \neq s(n)$

Proof. Let $S = \{n \in \mathbb{N}_0 | n \neq s(n)\}$ then we have

$0 \in S$. By [theorem: 5.10] $0 \neq s(0)$.

$n \in S \Rightarrow s(n) \in S$. Assume that $s(s(n)) = s(n)$. As $s(s(n)) = s(n) \bigcup \{s(n)\}$ we have that $s(n) \in s(s(n)) = s(n)$, so $s(n) \in n \bigcup \{n\}$. As $n \in S$ we have that $n \neq s(n)$ so we must have that $s(n) \in n$. As by [theorem: 5.14] $s(n)$ is transitive it follows that $s(n) \subseteq n$, further we have that $n \subseteq n \bigcup \{n\} = s(n)$. So we conclude that $n = s(n)$ proving $n \notin S$ which contradicts $n \in S$. So we must have that $s(s(n)) \neq s(n)$ proving that $s(n) \in S$.

Using mathematical induction it follows then that $\mathbb{N}_0 = S$ so if $n \in \mathbb{N}_0$ then $n \in S$ and thus $n \neq s(n)$. □

The next theorem shows that the successor function is a injection.

Theorem 5.16. *If* $n, m \in \mathbb{N}_0$ *is such that* $s(n) = s(m)$ then $n = m$. *In other words*

$$s: \mathbb{N}_0 \rightarrow \mathbb{N}_0 \text{ is injective}$$

Proof. As $n \in n \bigcup \{n\} = s(n) = s(m)$ and $m \in m \bigcup \{m\} = s(m) = s(n)$ we have that $n \in s(m) \wedge m \in s(n)$. Using [theorem: 5.12] this becomes

$$(n \in m \vee n = m) \wedge (m \in n \vee n = m) \Rightarrow (n \in m \wedge m \in n) \vee n = m$$

If $n = m$ we are done. So we must look at the case that $m \in n \wedge n \in m$. By transitivity [theorem: 5.14] we have then $n \subseteq m$ and $m \subseteq n$ proving that $n = m$. □

The above theorems are part of what is in number theory the Peano Axioms.

Theorem 5.17. (Peano Axioms) $\mathbb{N}_0$ *satisfies the following so called Peano Axioms*

1. $0 \in \mathbb{N}_0$
2. *If* $n \in \mathbb{N}_0$ *then* $s(n) \in \mathbb{N}_0$
3. $\forall n \in \mathbb{N}_0$ *we have that* $s(n) \neq 0$
4. *If* $X \subseteq \mathbb{N}_0$ *is such that*
   a. $0 \in X$
   b. $n \in X \Rightarrow s(n) \in X$

   then $X = \mathbb{N}_0$
5. *If* $n, m \in \mathbb{N}_0$ *is such that* $s(n) = s(m)$ *then* $n = m$

Proof.

1. See [theorem: 5.7]
2. See [definition: 5.6]
3. See [theorem: 5.10]
4. See [theorem: 5.11]
5. See [theorem: 5.16] □

Theorem 5.18. *If* $n \in \mathbb{N}_0 \wedge n \neq 0$ *then* $\exists! m \in \mathbb{N}_9$ *such that* $n = s(m)$

Proof. We use mathematical induction to prove this. So let

$$S = \{n \in \mathbb{N}_0 | (n = 0) \vee (\exists! m \in \mathbb{N}_0 \text{ such that } n = s(m))\} \subseteq \mathbb{N}_0$$

then we have:

$0 \in S$. As $0 = 0$ we have that $0 \in S$.

$n \in S \Rightarrow s(n) \in S$. Consider $s(n)$ then by [theorem: 5.10] $s(n) \neq 0$, further we have that $m = n$ satisfies $s(n) = s(m)$ proving the existance part. Assume that there is another $m' \in \mathbb{N}_0$ such that $s(n) = s(m')$, then by [theorem: 5.16] we have $n = m'$, proving uniqueness. So $s(n) \in S$.

Mathematical induction [see: 5.11] proves then that $\mathbb{N}_0 = S$. So if $n \in \mathbb{N}_0$ with $n \neq 0$ we have as $n \in S$ that $\exists! m \in \mathbb{N}_0$ such that $n = s(m)$. □

5.2 Recursion

Recursion will be used to essential define things in terms of itself. It is the mathematical eqivalent of iteration in many programming languages. Actually, functional languages that are mathematical oriented, like Haskell, have no iteration and loop constructs at all and relay fully on recursion. Recursion is based on the definition of a recursive function that takes the role of iterating. The following theorem ensures the existance of such a function.

Theorem 5.19. (Recursion) *Let A be a set, $a \in A$ and $f: A \rightarrow A$ a function then there exists a* ***unique*** *function*

$$\lambda: \mathbb{N}_0 \rightarrow A$$

such that

1. $\lambda(0) = a$
2. $\forall n \in \mathbb{N}_0$ *we have* $\lambda(s(n)) = f(\lambda(n))$

Proof. Define

$$\mathcal{G} = \{G | G \subseteq \mathbb{N}_0 \times A \text{ such that } (0, a) \in G \text{ and} \forall n \in \mathbb{N}_0 \text{ that } (n, x) \in G \Rightarrow (s(n), f(x)) \in G\}$$

Define $G = \mathbb{N}_0 \times A$ then as $0 \in \mathbb{N}_0$ and $a \in A$ we have $(0, a) \in \mathbb{N}_0 \times A$. Further if $(n, x) \in \mathbb{N}_0 \times A$ then $n \in \mathbb{N}_0$ and $x \in A$ so that $s(n) \in \mathbb{N}_0$ and $f(x) \in A$, hence $(s(n), f(x)) \in \mathbb{N}_0 \times A$. So

$$\mathbb{N}_0 \times A \in \mathcal{G} \tag{5.1}$$

We prove now that

$$\text{If } \lambda = \bigcap \mathcal{G} \text{ then } \lambda \in \mathcal{G},\ \lambda \subseteq N_0 \times A \text{ and } (0, a) \in \lambda \tag{5.2}$$

Proof.

1. By [eq: 5.1] we have $\mathbb{N}_0 \times A \in \mathcal{G}$ so that by [theorem: 1.60] $\bigcap \mathcal{G} \subseteq \mathbb{N}_0 \times A$ hence $\lambda \subseteq \mathbb{N}_0 \times A$
2. $\forall G \in \mathcal{G}$ we have by definition that $(0, a) \in G$ hence $(0, a) \in \bigcap \mathcal{G}$ or $(0, a) \in \lambda$
3. If $(n, x) \in \bigcap \mathcal{G}$ then $\forall G \in \mathcal{G}$ we have $(n, x) \in G \Rightarrow (s(n), f(x)) \in G$, so that $(s(n), f(x)) \in \bigcap \mathcal{G}$.

Using (1),(2) and (3) it follows that $\bigcap \mathcal{G} \in \mathcal{G}$. □

If $x \in \text{dom}(\lambda)$ then $\exists y$ such that $(x, y) \in \lambda \subseteq \mathbb{N}_0 \times A$ [see eq: 5.2] so that $x \in \mathbb{N}_0$, hence

$$\text{dom}(\lambda) \subseteq \mathbb{N}_0 \tag{5.3}$$

As by [eq: 5.2] $(0, a) \in \lambda$ we have that

$$0 \in \text{dom}(\lambda) \tag{5.4}$$

If $n \in \text{dom}(\lambda)$ then then $\exists x$ such that $(n, x) \in \lambda$, as by [eq: 5.2] $\lambda \in \mathcal{G}$, we have $(s(n), f(x)) \in \lambda$ so that $s(n) \in \text{dom}(\lambda)$. In other words we have

$$\text{if } n \in \text{dom}(\lambda) \text{ then } s(n) \in \text{dom}(\lambda) \tag{5.5}$$

Now [eq: 5.3], [eq: 5.4] and [eq: 5.5] are the conditions for mathematical induction [theorem: 5.11], so we have proved that

$$\text{dom}(\lambda) = \mathbb{N}_0 \tag{5.6}$$

We use now mathematical induction to prove that λ is the graph of a function. Let

$$S = \{n \in \mathbb{N}_0 | \exists! x \text{ such that } (n, x) \in \lambda\} \subseteq \mathbb{N}_0$$

then we have:

$0 \in S$. By [eq: 5.2] we have $(0, a) \in \lambda$. Assume that $\exists x \in A$ with $x \neq a$ such that $(0, x) \in \lambda$, then $(0, a) \neq (0, x)$. Define now $\beta = \lambda \setminus \{(0, x)\}$ then we have

1. $\beta \subseteq \lambda \subseteq \mathbb{N}_0 \times A$
2. As $(0, a) \neq (0, x)$ and $(0, a) \in \lambda$ we have $(0, a) \in \beta$
3. If $(n, y) \in \beta \underset{\beta \subseteq \lambda}{\Rightarrow} (n, y) \in \lambda$ so that $(s(n), f(x)) \in \lambda$, as by [theorem: 5.10] $s(n) \neq 0$ we have that $(s(n), f(x)) \neq (0, x)$, hence $(s(n), f(y)) \in \beta$

From (1),(2) and (3) it follows that $\beta \in \mathcal{G}$ so that by [theorem: 1.60] $\lambda = \bigcap \mathcal{G} \subseteq \mathcal{B}$ which as $(0, x) \in \lambda$ would give $(0, x) \in \beta = \lambda \setminus \{(0, x)\}$ a contradiction. So the assumption is wrong and we must have that $x = a$, proving uniqueness, hence that $0 \in S$.

$n \in S \Rightarrow s(n) \in S$. As $n \in S$ there exist a **unique** $x \in \mathcal{S}$ such that $(n, x) \in \lambda$. As $(n, x) \in \lambda$ we have as $\lambda \in \mathcal{G}$ that $(s(n), f(x)) \in \lambda$. Assume now that $\exists y$ such that $(s(n), y) \in \lambda$ and $f(x) \neq y$. Define then $\beta = \lambda \setminus \{(s(n), y)\}$ then we have:

1. $\beta \subseteq \lambda \subseteq \mathbb{N}_0 \times A$
2. As by [theorem: 5.15] $s(n) \neq 0$ we have that $(0, a) \neq (s(n), y)$, as further $(0, a) \in \lambda$ it follows that $(0, a) \in \beta$
3. If $(m, z) \in \beta$ then $(m, z) \in \lambda$ so that $(s(m), f(z)) \in \lambda$ we must now consider two cases for $s(n), s(m)$:

   $s(m) = s(n)$. Then by [theorem: 5.16] we have $n = m$ so that $(n, z) = (m, z) \in \lambda$. As $n \in S$ and we have $(n, x) \in \lambda$ it follows that $z = x$. So that $(s(m), f(z)) = (s(n), f(x)) \neq (s(n), y)$ [as we assumed that $y \neq f(x)$] hence we have that $(s(m), f(z)) \in \beta$.

   $s(m) \neq s(n)$. then $(s(m), f(z)) \neq (s(n), y)$ so that $(s(m), f(z)) \in \beta$

   So we have prove that if $(m, z) \in \beta$ then $(s(m), f(z)) \in \beta$

From (1),(2) and (3) it follows that $\beta \in \mathcal{G}$ but then using [theorem: 1.60] we have that $\lambda = \bigcap \mathcal{G} \subseteq \beta$ which as $(s(n), y) \in \lambda$ leads to $(s(n), y) \in \beta = \lambda \setminus \{(s(n), y)\}$ a contradiction. So the assumption is wrong and we must have that $y = f(x)$ proving **uniqueness**, hence we have that $s(n) \in S$.

Using mathematical induction [theorem: 5.11] it follows that $\mathbb{N}_0 = S$. So if $(n, x), (n, x') \in \lambda$ then $n \in \mathbb{N}_0 = S$ so that $y = y'$ giving

$$\text{If } (n, x), (n, x') \in \lambda \text{ then } x = x' \tag{5.7}$$

From [eq: 5.2], [eq: 5.6] and [eq: 5.7] it follows that

$$\lambda: \mathbb{N}_0 \to A \text{ is a function} \tag{5.8}$$

As $\lambda \in \mathcal{G}$ we have that $(0, a) \in \lambda \Rightarrow a = \lambda(0)$, further if $n \in \mathbb{N}_0 = \mathrm{dom}(\lambda)$ then $\exists x$ such that $(n,x) \in \lambda$ and $(s(n), f(x)) \in \lambda$, Now $(n, x) \in \lambda$ is equivalent with $\lambda(n) = x$ and $(s(n), f(x)) \in \lambda$ is equivalent with $\lambda(s(n)) = f(x) = f(\lambda(n))$. So we have for λ that

$$\lambda(0) = a \text{ and } \forall n \in \mathbb{N}_0 \text{ we have } \lambda(s(n)) = f(\lambda(n)) \tag{5.9}$$

So we have proved the existance of our function, next we must prove that this function is unique. Assume that there exist another function

$$\beta: \mathbb{N}_0 \to A \text{ such that } \beta(0) = a \text{ and } \forall n \in \mathbb{N}_0 \text{ we have } \lambda(s(n)) = f(\lambda(n))$$

We proceed by mathematical induction, so define $T=\{n\in\mathbb{N}_0|\lambda(n)=\beta(\lambda)\}$ then we have

$0\in T$. As $\lambda(0)=a=\beta(0)$ we have that $0\in T$.

$n\in T\Rightarrow s(n)\in T$. As $n\in T$ we have $\lambda(n)=\beta(n)$ but then $\lambda(s(n))=f(\lambda(n))=\beta(s(n))$ so that $s(n)\in T$

Using mathematical induction [theorem: 5.11] we have then $T=\mathbb{N}_0$. So $\forall n\in\mathbb{N}_0$ we have $n\in T$ hence $\lambda(n)=\beta(n)$ which by [theorem: 2.36] proves that

$$\lambda=\beta$$ □

Corollary 5.20. *If A is a set, $a\in A$ and $f: A\rightarrow A$ a function then there exists a unique function*

$$\lambda: \mathbb{N}_0\rightarrow A$$

such that

1. $\lambda(0)=a$
2. $\forall n\in\mathbb{N}_0$ *we have* $\lambda(s(n))=f(\lambda(n))$
3. *If* $a\notin f(A)$ *and* $f: A\rightarrow A$ *is injective then* λ *is injective*

Proof. The first part is easy. Using recursion [theorem: 5.19] there exists a function

$$\lambda: \mathbb{N}_0\rightarrow A$$

such that

$$\lambda(0)=a \text{ and } \forall n\in\mathbb{N}_0 \text{ we have } \lambda(s(n))=f(\lambda(n))$$

We use now mathematical induction to prove (3). Assume that $a\notin f(A)$ and take

$$S=\{n\in\mathbb{N}_0|\forall m\in\mathbb{N}_0 \text{ with } \lambda(n)=\lambda(m) \text{ we have n=m}\}$$

then we have:

$0\in S$. If $\lambda(m)=\lambda(0)$ then as $\lambda(0)=a$ we have that $\lambda(m)=a$. Assume that $m\neq 0$ then by [theorem: 5.18] there exists a $k\in\mathbb{N}_0$ such that $m=s(k)$ so that $a=\lambda(m)=\lambda(s(k))=f(\lambda(k))$, which proves that $a\in f(A)$ contradicting $a\notin f(A)$. Hence we must have $m=0$ so that $0\in S$.

$n\in S\Rightarrow s(n)\in S$. Let $m\in\mathbb{N}_0$ such that $\lambda(s(n))=\lambda(m)$. Assume that $m=0$ then $\lambda(s(n))=\lambda(m)=\lambda(0)=a$ so that $f(\lambda(n))=\lambda(s(n))=a$, resulting in $a\in f(A)$ contradicting $a\notin f(A)$. Hence we must have that $m\neq 0$. Using [theorem: 5.18] there exists a $k\in\mathbb{N}_0$ such that $m=s(k)$, from $\lambda(s(n))=\lambda(m)$ it follows then that $\lambda(s(n))=\lambda(s(k))$ so that $f(\lambda(n))=\lambda(s(n))=\lambda(s(k))=f(\lambda(k))$. As f is injective we have $\lambda(n)=\lambda(k)$. Now as $n\in S$ we must have $n=k$ or $s(n)=s(k)=m$. This proves that $\forall m\in\mathbb{N}_0$ with $\lambda(s(n))=\lambda(m)$ we have $s(n)=m$, hence $s(n)\in S$

Using mathematical induction [theorem: 5.11] it follows that $\mathbb{N}_0=S$. So if $n,m\in\mathbb{N}_0$ is such that $\lambda(n)=\lambda(m)$ then $n\in S$ and as $m\in\mathbb{N}_0$ we have $n=m$, proving that

$$\lambda \text{ is injective}$$ □

Remark 5.21. To understand how recursion works in the above theorem consider the following, Let $f: A\rightarrow A$ a function, $a\in A$ and $\lambda: \mathbb{N}_0\rightarrow A$ such that $\lambda(0)=a$ and $\lambda(s(n))=f(\lambda(n))$

$$\begin{array}{rcl}
\lambda(0) & = & a\\
\lambda(1)=\lambda(s(n)) & = & f(\lambda(0))=f(a)\\
\lambda(2)=\lambda(s(1)) & = & f(\lambda(1))=f(f(a))\\
\lambda(3)=\lambda(s(2)) & = & f(\lambda(2))=f(f(f(a)))\\
 & \ldots & \\
\lambda(n) & = & \overbrace{f(f(\ldots(f(a))))}^{\text{n times}}
\end{array}$$

so $\lambda(n)$ is the result of applying f n-times on a value a. If $a\notin f(A)$ and f is injective then λ is injective and we would have that $f(a), f(f(z)), f(f(f(a))),\ldots,\overbrace{f(f(\ldots(f(a))))}^{\text{n times}}$ are all different numbers.

To see the conditions for injectivity of λ consider the following two examples:

Example 5.22. Define $f:\{1,2,3\}\rightarrow f(\{1,2,3\})$ by $f(i)=\begin{cases}2 \text{ if } i=1\\ 3 \text{ if } i=2\\ 2 \text{ if } i=1\end{cases}$ (so f is not injective) and $a=3$

then we have

$$\begin{array}{rcl}\lambda(0) & = & 3\\ \lambda(1) & = & f(3)=2\\ \lambda(2) & = & f(f(3))=f(2)=1\\ \lambda(3) & = & f(f(f(3)))=f(1)=2\\ \lambda(4) & = & f(f(f(3)))=f(2)=1\\ & \ldots & \end{array}$$

So that $\lambda:\mathbb{N}_0-A$ is clearly not injective.

Example 5.23. Take $f:\{1,2,3\}\rightarrow\{1,2,3\}$ by $f(i)=\begin{cases}2 \text{ if } i=1\\ 3 \text{ if } i=2\\ 1 \text{ if } i=3\end{cases}$ so that f is injective and $a=2$ so that $a\in f(\{1,2,3\})$ then we have

$$\begin{array}{rcl}\lambda(0) & = & 2\\ \lambda(1) & = & f(2)=1\\ \lambda(2) & = & f(f(2))=f(1)=2\\ \lambda(3) & = & f(f(f(2)))=f(2)=1\\ & \ldots & \end{array}$$

So that $\lambda:\mathbb{N}_0\rightarrow\{1,2,3\}$ is not injective.

We can rephrase the above remark in the iteration principle that is useful in proofs using mathematical induction.

Theorem 5.24. (Iteration) *Let A be a non empty set and $f:A\rightarrow A$ a function. Then $\forall n\in\mathbb{N}_0$ there exist a* ***unique*** *function*

$$(f)^n: A\rightarrow A$$

such that

1. $(f)^0=\mathrm{Id}_A$
2. $(f)^{s(n)}=f\circ(f)^n$

Proof. Let $a\in A$ and use the recursion [theorem: 5.19] to find a function

$$\lambda_a:\mathbb{N}_0\rightarrow A \text{ such that } \lambda_a(0)=a \text{ and } \forall n\in\mathbb{N}_0\ \lambda_a(s(n))=f(\lambda_a(n))$$

Define now

$$(f)^n: A\rightarrow A \text{ where } (f)^n(a)=\lambda_a(n)$$

Then we have

1. $\forall a\in A$ we have that $(f)^0(a)=\lambda_a(0)=a$ so that

$$(f)^0=\mathrm{Id}_A$$

2. $\forall a \in A$ we have that $(f)^{s(n)}(a) = \lambda_a(s(n)) = f(\lambda_a(n)) = f((f)^n(a)) = (f \circ (f)^n)(a)$ so that

$$(f)^{s(n)} = f \circ (f)^n$$

□

As illustration of iteration let $f: A \rightarrow A$ then we have

$$\begin{array}{rcl} (f)^0 & = & \mathrm{Id}_A \\ (f)^1 = (f)^{s(0)} & = & f \circ (f)^0 = f \circ \mathrm{Id}_A = f \\ (f)^2 = (f)^{s(1)} & = & f \circ (f)^1 = f \circ f \\ (f)^3 = (f)^{s(2)} & = & f \circ (f)^2 = f \circ f \circ f \\ & \ldots & \\ (f)^n & = & \overbrace{f \circ \ldots \circ f}^{n\,\text{times}} \end{array}$$

We can apply the above on a group to define new operations on the group.

Example 5.25. Let $\langle A, \oplus \rangle$ be a group and $a \in A$ define then $\oplus_a: A \rightarrow A$ by $x \rightarrow \oplus_a(x) = x \oplus a$ we define then given $n \in \mathbb{N}$ $a\langle\oplus\rangle n = (\oplus_a)^n(e)$ where e is the neutral element in the group . So

$$\begin{array}{rcl} a\langle\oplus\rangle 0 & = & (\oplus_a)^0(e) = \mathrm{Id}_A(e) = e \\ a\langle\oplus\rangle 1 & = & (\oplus_a)^1(e) = \oplus_a(e) = a \oplus e = e \\ a\langle\oplus\rangle 2 & = & (\oplus_a)^2(e) = \oplus_a(\oplus_a(e)) = a \oplus (a \oplus e) = a \oplus (a \oplus e) = a \oplus a \\ a\langle\oplus\rangle 3 & = & (\oplus_a)^3(e) = (\oplus_a(\oplus_a(\oplus_a(e)))) = a \oplus (a \oplus (a \oplus e)) = a \oplus a \oplus a \\ & \ldots & \\ a\langle\oplus\rangle n & = & \overbrace{a \oplus \cdots \oplus a}^{\text{n times}} \end{array}$$

Sometimes we consider a group to be additive or multiplicative, this is either noted as $\langle A, + \rangle$ with neutral element 0 or $\langle A, \cdot \rangle$ with neutral element 1. Then we note $a\langle+\rangle n$ as $a \cdot n$ as and $a\langle\cdot\rangle n$ as a^n hence we have

1. Additive group $\langle A, + \rangle$ with neutral element 0 gives

$$\begin{array}{rcl} a \cdot 0 & = & 0 \\ a \cdot 1 & = & a \\ a \cdot 2 & = & a+a \\ a \cdot 3 & = & a + a + a \\ & \ldots & \\ a \cdot n & = & \overbrace{a + \cdots + a}^{\text{n times}} \end{array}$$

2. Multiplicative group $\langle A, \cdot \rangle$ with neutral element 1 gives

$$\begin{array}{rcl} a^0 & = & 1 \\ a^1 & = & a \\ a^2 & = & a \cdot a \\ a^3 & = & a \cdot a \cdot a \\ & \ldots & \\ a^n & = & \overbrace{a \cdot \cdots \cdot a}^{\text{n times}} \end{array}$$

Recursion is mostly used in it's step form to define recursive functions.

Theorem 5.26. (Recursion on $\mathbb{N}_0$ Step Form) *Let A be a set, $a \in A$ and $g: \mathbb{N} \times A \rightarrow A$ a function then there exist a **unique** function $\lambda: \mathbb{N}_0 \rightarrow A$ such that*

1. $\lambda(0) = a$
2. $\forall n \in \mathbb{N}_0$ *we have* $\lambda(s(n)) = g(n, \lambda(n))$

Proof. First we define the projection functions

$$\pi_1: \mathbb{N}_0 \times A \rightarrow \mathbb{N}_0 \text{ where } \pi_1(n, x) = n$$

$$\pi_2: \mathbb{N}_0 \times A \rightarrow A \text{ where } \pi_2(n, x) = x$$

Define now

$$\gamma: \mathbb{N}_0 \times A \rightarrow \mathbb{N}_0 \times A \text{ where } \gamma(x) = (s(\pi_1(x)), g(\pi_1(x), \pi_2(x))) \tag{5.10}$$

Using the iteration [theorem: 5.24] on the above functions gives $\forall n \in \mathbb{N}_0$ the existance of the function

$$(\gamma)^n: \mathbb{N}_0 \times A \rightarrow \mathbb{N}_0 \times A \text{ such that } (\gamma)^0 = \mathrm{Id}_{\mathbb{N}_0 \times A} \text{ and } \forall n \in \mathbb{N}_0 \text{ we have } (\gamma)^{s(n)} = \gamma \circ (\gamma)^n \tag{5.11}$$

We prove now by mathematical induction that $\forall n \in \mathbb{N}_0$ $\pi_1((\gamma)^n(0, a)) = n$. So let

$$S = \{n \in \mathbb{N}_0 | \pi_1((\gamma)^n(0, a)) = n\}$$

then we have:

$0 \in S$. As $\pi_1((\gamma)^0(0, a)) \underset{[\text{eq: } 5.11]}{=} \pi_1(\mathrm{Id}_{\mathbb{N}_0 \times A}(0, a)) = \pi_1(0, a) = 0$ we have that $0 \in S$

$n \in S \Rightarrow s(n) \in S$. We have

$$\begin{aligned}
\pi_1((\gamma)^{s(n)}(0, a)) &\underset{[\text{eq: } 5.11]}{=} \pi_1((\gamma \circ (\gamma)^n)(0, a)) \\
&= \pi_1(\gamma((\gamma)^n(0, n))) \\
&\underset{[\text{eq: } 5.10]}{=} \pi_1(\pi_1((\gamma)^n(0, n)), g(\pi_1((\gamma)^n(0, a)), \pi_2((\gamma)^n(0, a)))) \\
&\underset{n \in S \Rightarrow \pi_1((\gamma)^n(0,a)) = n}{=} \pi_1(n, g(n, \pi_2((\gamma)^n(0, a)))) \\
&= n
\end{aligned}$$

proving that $s(n) \in S$

Using mathematical induction [theorem: 5.11] we have $\mathbb{N}_0 = S$, hence

$$\forall n \in \mathbb{N}_0 \text{ we have } \pi_1((\gamma)^n(0, a)) = n \tag{5.12}$$

Define now

$$\lambda: \mathbb{N}_0 \rightarrow A \text{ by } \gamma(n) = \pi_2((\gamma)^n(0, a)) \tag{5.13}$$

then we have:

1. $\lambda(0) = \pi_2((\gamma)^0(0, a)) = \pi_2(\mathrm{Id}_{\mathbb{N}_0 \times A}(0, a)) = \pi_2(0, a) = a$
2. If $n \in \mathbb{N}_0$ then

$$\begin{aligned}
\lambda(s(n)) &= \pi_2((\gamma)^{s(n)}(0, a)) \\
&\underset{[\text{eq: } 5.11]}{=} \pi_2((\gamma \circ (\gamma)^n)(0, a)) \\
&= \pi_2(\gamma((\gamma)^n(0, a))) \\
&\underset{[\text{eq: } 5.10}{=} \pi_2(\pi_1((\gamma)^n(0, a)), g(\pi_1((\gamma)^n(0, a)), \pi_2((\gamma)^n(0, a)))) \\
&= g(\pi_1((\gamma)^n(0, a)), \pi_2((\gamma)^n(0, a))) \\
&\underset{[\text{eq: } 5.12}{=} g(n, \pi_2((\gamma)^n(0, a))) \\
&\underset{[\text{eq: } 5.13}{=} g(n, \lambda(n))
\end{aligned}$$

This proves the existance of the function we are searching for. Now for uniqueness assume that there is a

$$\beta: \mathbb{N}_0 \rightarrow A \text{ such that } \beta(0) = a \text{ and } \forall n \in \mathbb{N}_0 \text{ that } \beta(s(n)) = g(n, \beta(n))$$

Define now $B = \{n \in \mathbb{N}_0 | \lambda(n) = \beta(n)\}$ then we have:

$0 \in B$. As $\beta(0) = a = \lambda(0)$ it follows that $0 \in B$.

$n \in B \Rightarrow s(n) \in B$. As

$$\beta(s(n)) = g(n, \beta(n)) \underset{n \in B}{=} g(n, \lambda(n)) = \lambda(s(n))$$

we have that $s(n) \in B$

Using mathematical induction we have $B = \mathbb{N}_0$, so $\forall n \in \mathbb{N}_0$ we have $n \in B$ hence $\beta(n) = \lambda(n)$ proving that

$$\beta = \lambda$$

□

Up to now we have used the successor function $s: \mathbb{N}_0 \rightarrow \mathbb{N}_0$ in the recursion and induction theorems. Once we have introduced the arithmetic of the natural numbers, we wil rewrite these theorems by a version where $s(n)$ is replaced by $n + 1$.

5.3 Arithmetic of the Natural numbers

We use recursion to define the sum of two natural numbers.

Definition 5.27. *Let $m, n \in \mathbb{N}_0$ then the addition operator $+$ is defined by*

$$+: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0 \text{ where } n + m \underset{notation}{=} +(n, m) = (s)^m(n)$$

Here $s: \mathbb{N}_0 \rightarrow \mathbb{N}_0$ is the successor function [definition: 5.6] and we use the iteration principle from [theorem: 5.24] to define $(s)^n$.

Example 5.28. Using this definition we can easely calculate that $1 + 1 = 2$

Proof. $1 + 1 = (s)^1(1) = (s \circ (s)^0)(s) = s((s)^0(1)) = s(\mathrm{Id}_{\mathbb{N}_0}(1)) = s(1) = 2$ □

We will show now that $\langle \mathbb{N}_0, + \rangle$ forms a abelian semi-group.

Theorem 5.29. (Neutral Element) *Let $n \in \mathbb{N}_0$ then $n + 0 = n = 0 + n$*

Proof.

1. $n + 0 = (s)^0(n) = \mathrm{Id}_{\mathbb{N}_0}(n) = n$
2. For the $0 + n = n$ we use mathematical induction. So let $S = \{n \in \mathbb{N}_0 | 0 + n = n\}$ then we have:

   $0 \in S$. As $0 + 0 \underset{(1)}{=} 0$ proving $0 \in S$

   $n \in S \Rightarrow s(n) \in S$. We have $0 + s(n) = (s)^{s(n)}(0) = (s \circ (s)^n)(0) = s((s)^n(0)) \underset{n \in S}{=} s(n)$ proving that $s(n) \in S$

   Using mathematical induction 5.11 we have $S = \mathbb{N}_0$. So if $n \in \mathbb{N}_0 \Rightarrow n \in S$ then $0 + n = n$. □

Theorem 5.30. *$\forall n \in \mathbb{N}_0$ we have $n + 1 = s(n) = 1 + n$*

Proof.

1. $n + 1 = (s)^1(n) = (s \circ (s)^0)(n) = s((s)^0(n)) = s(\mathrm{Id}_{\mathbb{N}_0}(n)) = s(n)$
2. For $1 + n = s(n)$ we use induction, so define $S = \{n \in \mathbb{N}_0 | 1 + n = s(n)\}$ then we have:

   $0 \in S$. $1 + 0 \underset{\text{[theorem: 5.29]}}{=} 1 = s(0)$

   $n \in S \Rightarrow n + 1 \in S$.

$$1 + s(n) = (s)^{s(n)}(1) = (s \circ (s)^n)\,(1) = s((s)^n(1)) = s(1 + n) \underset{n \in S}{=} s(s(n))$$

proving that $s(n) \in S$.

By mathematical induction [theorem: 5.11] we have $S = \mathbb{N}_0$ completing the proof. □

Lemma 5.31. *If $n, m \in \mathbb{N}$ then $n+s(m) = s(n+m)$*

Proof. $n+s(m) = (s)^{s(m)}(n) = (s \circ (s)^m)(n) = s((s)^m(n)) = s(n+m)$ □

Theorem 5.32. (Associativity) *If $n, m, k \in \mathbb{N}$ then $(n+m)+k = n+(m+k)$*

Proof. The proof is by mathematical induction, so given $n, m \in \mathbb{N}_0$ define

$$S_{n,m} = \{k \in \mathbb{N} | (n+m)+k = n+(m+k)\}$$

then we have:

$0 \in S_{n,m}$. $(n+m)+0 \underset{\text{[theorem: 5.29}}{=} n+m \underset{\text{[theorem: 5.29}}{=} n+(m+0) \Rightarrow 0 \in S_{n,m}$

$k \in S_{n,m} \Rightarrow s(k) \in S_{n,m}$. We have

$$\begin{aligned}(n+m)+s(k) &\underset{\text{[lemma: 5.31}}{=} s((n+m)+k)\\ &\underset{k \in S}{=} s(n+(m+k))\\ &\underset{\text{[lemma: 5.31}}{=} (n+s(m+k))\\ &\underset{\text{[lemma: 5.31}}{=} (n+(m+s(k)))\end{aligned}$$

proving that $s(k) \in S_{n,m}$.

By mathematical induction [theorem: 5.11] we have $\mathbb{N}_0 = S_{n,m}$. So if $n, m, k \in \mathbb{N}_0$ then $k \in S_{n,m} \Rightarrow (n+m)+k = n+(m+k)$ □

Theorem 5.33. (Commutativity) *If $n, m \in \mathbb{N}$ then $n+m = m+n$*

Proof. This is done again by induction. Let $n \in \mathbb{N}_0$ and define

$$S_n = \{k \in \mathbb{N}_0 | n+k = k+n\}$$

then we have:

$0 \in S_n$. Using [theorem: 5.29] it follows that $n+0 = 0+n$ proving that $0 \in S_n$

$k \in S_n \Rightarrow s(k) \in S_n$. We have

$$\begin{aligned}n+s(k) &\underset{\text{[lemma: 5.31}}{=} s(n+k)\\ &\underset{k \in S_{n,m}}{=} s(k+n)\\ &\underset{\text{[theorem: 5.30}}{=} 1+(k+n)\\ &\underset{\text{[theorem: 5.32}}{=} (1+k)+n\\ &\underset{\text{[theorem: 5.30}}{=} s(k)+n\end{aligned}$$

Using mathematical induction [theorem: 5.11] we have that $S_n = \mathbb{N}_0$, So if $n, m \in \mathbb{N} \Rightarrow m \in S_n \Rightarrow n+m = m+n$. □

We can summarize the above theorems as follows.

Theorem 5.34. *$\langle \mathbb{N}_0, + \rangle$ forms a Abelian semi-group with neutral element 0*

Proof.

neutral element. This follows from [theorem: 5.29].

associativity. This follows from [theorem: 5.32].

commutativity. This follows from [theorem: 5.33] □

Next we use recursion to define multiplication in $\mathbb{N}_0$ and prove that $\langle \mathbb{N}_0, \cdot \rangle$ is a abelian group.

Definition 5.35. (Multiplication) *Given $n \in \mathbb{N}_0$ define*

$$\alpha_n: \mathbb{N}_0 \rightarrow \mathbb{N}_0 \text{ by } \alpha_n(m) = n + m$$

Then we define the multiplication operator as follows

$$\cdot: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0 \text{ by } n \cdot m = .(n, m) = (\alpha_n)^m(0)$$

Using the above definition we have
We have the following examples to see how multiplication works by repeating summation

$$\begin{array}{lcl}
2 \cdot 0 & = & (\alpha_2)^0(0) = \mathrm{Id}_{\mathbb{N}}(0) = 0 \\
2 \cdot 1 & = & (\alpha_2)^1(0) = (\alpha_2)^{s(0)}(0) = (\alpha_2 \circ (\alpha_2)^0)(0) = \alpha_2(0) = 2+0 = 2 \\
2 \cdot 2 & = & (\alpha_2)^2(0) = (\alpha_2)^{s(1)}(0) = (\alpha_2((\alpha_2)^1(0))) = \alpha_2(2) = 2+2 = 4 \\
& \ldots. &
\end{array}$$

Theorem 5.36. (Absorbing Element) *If $n \in \mathbb{N}_0$ then $n \cdot 0 = 0 = 0 \cdot n$*

Proof.

1. $n \cdot 0 = (\alpha_n)^0(0) = \mathrm{Id}_{\mathbb{N}_0}(0) = 0$
2. We prove by induction that $0 \cdot n = 0$, so let $S = \{n \in \mathbb{N}_0 | 0 \cdot n = 0\}$ then we have:

   $0 \in S$. This follows from $0 \cdot 0 \underset{(1)}{=} 0$

   $n \in S \Rightarrow s(n) \in S$. We have

$$\begin{array}{rcl}
0 \cdot s(n) & = & (\alpha_0)^{s(n)}(0) \\
& = & (\alpha \circ (\alpha_0)^n)(0) \\
& = & \alpha_0((\alpha_0)^n(0)) \\
& = & \alpha_0(0 \cdot n) \\
& \underset{n \in S}{=} & \alpha_0(0) \\
& = & 0 + 0 \\
& \underset{\text{[theorem: 5.29}}{=} & 0
\end{array}$$

   proving that $s(n) \in \mathcal{S}$.

   By induction [theorem: 5.11] we have that $S = \mathbb{N}_0$ hence the theorem follows. □

Theorem 5.37. (Neutral Element) *If $n \in \mathbb{N}_0$ then $n \cdot 1 = n = 1 \cdot n$*

Proof.

1.

$$\begin{array}{rcl}
n \cdot 1 & = & (\alpha_n)^1(0) \\
& = & (\alpha_n)^{s(0)}(0) \\
& = & (\alpha_n \circ (\alpha_n)^0)(0) \\
& = & \alpha_n((\alpha_n)^0(0)) \\
& = & \alpha_n(\mathrm{Id}(0)) \\
& = & \alpha_n(0) \\
& = & n + 0 \\
& \underset{\text{[theorem: 5.29]}}{=} & n
\end{array}$$

2. We prove $1 \cdot n$ by induction, so let $S = \{n \in \mathbb{N}_0 | 1 \cdot n = n\}$ then we have:

   $0 \in S$. This follows from $1 \cdot 0 \underset{\text{[theorem: 5.36]}}{=} 0$

   $n \in S \Rightarrow s(n) \in S$. We have

$$\begin{array}{rcl} 1 \cdot s(n) & = & (\alpha_1)^{s(n)}(n) \\ & = & (\alpha_1 \circ (\alpha_1)^n)(0) \\ & = & a_1((\alpha_1)^n(0)) \\ & = & \alpha_1(1 \cdot n) \\ & \underset{n \in S}{=} & \alpha_1(n) \\ & = & 1 + n \\ & \underset{\text{[theorem: 5.30}}{=} & s(n) \end{array}$$

   proving that $s(n) \in S$.

   By induction [theorem: 5.11] it follows that $S = \mathbb{N}_0$ completing the proof. □

Lemma 5.38. *If $n, m \in \mathbb{N}_0$ then $n \cdot s(m) = n + n \cdot m \underset{\text{[theorem: 5.33]}}{=} n \cdot m + n$.*

Proof. $n \cdot s(m) = (\alpha_n)^{s(m)}(0) = (\alpha_n \circ (\alpha_n)^m)(0) = a_n((\alpha_n)^m(0)) = \alpha_n(n \cdot m) = n + n \cdot m$. □

Theorem 5.39. (Distributivity) *$\forall n, m, k \in \mathbb{N}_0$ we have $(n + m) \cdot k = n \cdot k + m \cdot k$.*

Proof. We use induction to prove this. So given $n, m \in \mathbb{N}_0$ let

$$S_{n,m} = \{k \in \mathbb{N}_0 | (n + m) \cdot k = n \cdot k + m \cdot k\}$$

then we have:

$0 \in S_{n,m}$. $(n + m) \cdot 0 \underset{\text{[theorem: 5.36]}}{=} 0 \underset{\text{[theorem: 5.29]}}{=} 0 + 0 \underset{\text{[theorem: 5.36]}}{=} n \cdot 0 + m \cdot 0$

$n \in S_{n,m} \Rightarrow s(n) \in S_{n,m}$. We have

$$\begin{array}{rcl} (n + m) \cdot s(k) & \underset{\text{[lemma: 5.38}}{=} & (n + m) \cdot k + (n + m) \\ & \underset{k \in S_{n,m}}{=} & (n \cdot k + m \cdot k) + (n + m) \\ & \underset{\text{[theorem: 5.32}}{=} & n \cdot k + (m \cdot k + (n + m)) \\ & \underset{\text{[theorem: 5.33]}}{=} & n \cdot k + (m \cdot k + (m + n)) \\ & \underset{\text{[theorem: 5.32}}{=} & n \cdot k + ((m \cdot k + m) + n) \\ & \underset{\text{[theorem: 5.33]}}{=} & n \cdot k + (n + (m \cdot k + m)) \\ & \underset{\text{[theorem: 5.32}}{=} & (n \cdot k + n) + (m \cdot k + m) \\ & \underset{\text{[lemma: 5.38}}{=} & n \cdot s(k) + m \cdot s(k) \end{array}$$

proving that $s(k) \in S_{n,m}$.

By induction [theorem: 5.11] it follows that $\mathbb{N}_0 = S_{n,m}$. So if $n, m, k \in \mathbb{N}_0$ then $k \in S_{n,m}$ giving $(n + m) \cdot k = n \cdot k + m \cdot k$. □

Theorem 5.40. (Commutativity) *If $n, m \in \mathbb{N}_0$ then $n \cdot m = m \cdot n$.*

Proof. We prove this by induction so given $n \in \mathbb{N}_0$ let $S_n = \{m \in \mathbb{N}_0 | n \cdot m = m \cdot n\}$ then we have:

$0 \in S_n$. Using [theorem: 5.36] we have $n \cdot 0 = 0 = 0 \cdot n$ proving that $0 \in S_n$.

$\boldsymbol{m \in S_n \Rightarrow s(m) \in S_n}$. We have

$$\begin{aligned} n \cdot s(m) &\underset{[\text{lemma: } 5.38}{=} n + n \cdot m \\ &\underset{m \in S_n}{=} n + m \cdot n \\ &\underset{[\text{theorem: } 5.37]}{=} 1 \cdot n + m \cdot n \\ &\underset{[\text{threorem } 5.39]}{=} (1+n) \cdot n \\ &\underset{[\text{theorem: } 5.30}{=} s(m) \cdot n \end{aligned}$$

proving that $s(m) \in S_n$.

Using induction [theorem: 5.11] it follows that $\mathbb{N}_0 = S_n$. So if $n, m \in \mathbb{N}_0$ then $m \in S_n$ hence $n \cdot m = m \cdot n$. □

Theorem 5.41. **(Associativity)** *If $n, m, k \in \mathbb{N}_0$ then $(n \cdot m) \cdot k = n \cdot (m \cdot k)$*

Proof. We prove this by induction. So given $n, m \in \mathbb{N}_0$ define

$$S_{n,m} = \{k \in \mathbb{N}_0 | (n \cdot m) \cdot k = n \cdot (m \cdot k)\}$$

then we have:

$\boldsymbol{0 \in S_{n,m}}$. This follows from $(n \cdot m) \cdot 0 \underset{[\text{theorem: } 5.36]}{=} 0 \underset{[\text{theorem: } 5.36]}{=} n \cdot 0 = \underset{[\text{theorem: } 5.36]}{=} n \cdot (m \cdot 0)$

$\boldsymbol{k \in S_{n,m} \Rightarrow s(k) \in S_{n,m}}$. We have

$$\begin{aligned} (n \cdot m) \cdot s(k) &\underset{[\text{theorem: } 5.38]}{=} (n \cdot m) \cdot k + n \cdot m \\ &\underset{k \in S_{n,m}}{=} n \cdot (m \cdot k) + n \cdot m \\ &\underset{[\text{theorem: } 5.40]}{=} (m \cdot k) \cdot n + m \cdot n \\ &\underset{[\text{theorem: } 5.39]}{=} ((m \cdot k) + m) \cdot n \\ &\underset{[\text{theorem: } 5.40]}{=} n \cdot ((m \cdot k) + m) \\ &\underset{[\text{theorem: } 5.38]}{=} n \cdot (m \cdot s(k)) \end{aligned}$$

proving that $s(k) \in S_{n,m}$.

Using induction we have then that $\mathbb{N}_0 = S_{n,m}$. So if $n, m, k \in \mathbb{N}_0$ we have $k \in S_{n,m}$ giving $(n \cdot m) \cdot k = n \cdot (m \cdot k)$. □

To summarize the above we have the following;

Theorem 5.42. *$\langle \mathbb{N}_0, \cdot \rangle$ is a abelian semi-group with neutral element 1.*

Proof.

neutral element. This follows from [theorem: 5.37]

associativity. This follows from [theorem: 5.41]

commutativity. This follows from [theorem: 5.40] □

Although there is no inverse element for addition in $\mathbb{N}_0$ [this will be solved by the set of whole numbers], we can still solve equations as is expressed in the next theorem.

Theorem 5.43. *If $n, m, k \in \mathbb{N}_0$ then if $n + k = m + k$ it follows that $n = m$*

Proof. We prove this by induction. So given $n, m \in \mathbb{N}_0$ define $S = \{k \in \mathbb{N}_0 | \forall n, m \in \mathbb{N}_0$ with $n + k = m + k$ we have n=m$\}$ then we have:

$\boldsymbol{0 \in S}$. If $n, m \in \mathbb{N}_0$ are such that that $n + 0 = m + 0$ then we have $n \underset{5.29}{=} n + 0 = m + 0 \underset{5.29}{=} m$ or $n = m$ which proves that $0 \in S$

$k \in S \Rightarrow s(k) \in S$. If $n, m \in \mathbb{N}_0$ are such that $n + s(k) = m + s(k)$ then we have by [theorem: 5.30] that $n + (1 + k) = m + (1 + k)$ or using [theorem: 5.32] that $(n + 1) + k = (m + 1) + k$. As $k \in S$ it follows that $n + 1 = m + 1$ or using [theorem: 5.30] that $s(n) = s(m)$. Finally using [theorem: 5.16] we have $n = m$. So $s(k) \in S$.

Using induction we have then that $\mathbb{N}_0 = S$. So if $n, m, k \in \mathbb{N}_0$ then as $k \in S$ we have if $n + k = m + k$ that $n = m$. □

Note 5.44. We do not have a equivalent theorem for the product of two natural numbers, for example $0 \cdot 0 = 1 \cdot 0$ but we don't have that $1 = 0$.

5.4 Order relation on the natural numbers

Theorem 5.45. *If we define the relation $\leqslant$ by*

$$\leqslant = \{(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0 | n \in m \vee n = m\}$$

then

$$\langle \mathbb{N}_0, \leqslant \rangle \text{ is a partial ordered set}$$

Proof.

reflectivity. If $n \in \mathbb{N}_0$ then $n = n \Rightarrow n \in n \vee n = n$ so that $n \leqslant n$.

anti-symmetry. If $n \leqslant m \wedge m \leqslant n$ then we have

$$\begin{aligned}
(n \in m \vee n = m) \wedge (m \in n \vee m = n) &\Rightarrow (n \in m \vee n = m) \wedge (m \in n \vee n = m) \\
&\Rightarrow (n \in m \wedge m \in n) \vee n = m \\
&\underset{[\text{theorem: } 5.14]}{\Rightarrow} (n \subseteq m \wedge m \subseteq n) \vee n = m \\
&\Rightarrow n = m \vee n = m \\
&\Rightarrow n = m
\end{aligned}$$

transitivity. If $n \leqslant m \wedge m \leqslant k$ then we have the following possibilities to consider

1. $n \in m \wedge m \in k$ then by [theorem: 5.14] $n \in m \wedge m \subseteq k \Rightarrow n \in k \Rightarrow n \leqslant k$
2. $n \in m \wedge m = k$ then $n \in k$ so that $n \leqslant k$
3. $n = m \wedge m \in k$ then $n \in k$ so that $n \leqslant k$
4. $n = m \wedge m = k$ then $n = k \Rightarrow n \leqslant k$

So in all cases we have $n \leqslant k$ proving transitivity. □

Theorem 5.46. $\forall n \in \mathbb{N}_0$ *we have* $0 \leqslant n$

Proof. We prove this by induction, so let $S = \{n \in \mathbb{N}_0 | 0 \leqslant n\}$ then we have:

$0 \in S$. $0 = 0$ so that $0 \leqslant 0$ priving that $0 \in S$.

$n \in S \Rightarrow s(n) \in S$. As $s(n) = n \bigcup \{n\}$ we have that $n \in s(n)$ so that $n \leqslant s(n)$, as $n \in S$ $0 \leqslant n$, so by transitivity we have that $0 \leqslant s(n)$. Hence we have $s(n) \in S$.

Using induction [theorem: 5.11] it follows that $\mathbb{N}_0 = S$ proving the theorem. □

Theorem 5.47. $\forall n \in \mathbb{N}_0$ *we have* $n < s(n)$ *[in other words using [theorem: 5.30] we have* $n < n + 1$*]*

Proof. From $n \in n \bigcup \{n\} = s(n)$ we have that $n \leqslant s(n)$ and by [theorem: 5.15] $n \neq s(n)$ so that $n < s(n)$. □

Theorem 5.48. *If $n \in \mathbb{N}_0$ then $k \in n \Leftrightarrow k < n$.*

Proof.

$\Rightarrow$. We proceed by induction, so let $S = \{n \in \mathbb{N}_0 | \text{If } k \in n \Rightarrow k < n\}$ then we have:

$0 \in S$. As $0 = \varnothing$ so that $k \in 0$ is never true hence $k \in n \Rightarrow k < n$ is true, proving that $0 \in S$.

$n \in S \Rightarrow s(n) \in S$. If $k \in s(n) = n \bigcup \{n\}$ then we have the following cases to consider:

$k \in n$. As $n \in S$ we have $k < n$, further from [theorem: 5.47] we have $n < s(n)$ so that $k < s(n)$.

$k = n$. By [theorem: 5.47] we have $n < s(n)$ so that $k < s(n)$.

So in all cases we have $k < s(n)$ proving that $s(n) \in S$.

By the induction [theorem: 5.11] it follows that $\mathbb{N}_0 = S$, proving the theorem.

$\Leftarrow$. If $k < n$ then $k \neq n$ and $k \leqslant n \Rightarrow k \in n \vee k = n$ so that $k \in n$. □

Theorem 5.49. *If $n, m \in \mathbb{N}_0$ then we have that*

1. *$n < 0$ is false.*
2. *If $n \leqslant 0$ then $n = 0$.*
3. *$n < m \wedge m < n$ is false.*
4. *$n \leqslant m \wedge m < n$ is false.*
5. *$n < m \wedge m \leqslant n$ is false.*

Proof.

1. If $n < 0$ then by [theorem: 5.48] we have $n \in 0 = \varnothing$ which is false.
2. If $n \leqslant 0$ then we have either $n < 0$ [which by (1) is false] or $n = 0$.
3. If $n < m \wedge m < n$ then $n \leqslant m \wedge m \leqslant n \Rightarrow n = m$ and $n \neq m$ which is a contradiction.
4. If $n \leqslant m \wedge m < n$ then $n \leqslant m \wedge m \leqslant n \Rightarrow n = m$ and $n \neq m$ which is a contradiction.
5. If $n < m \wedge m \leqslant n$ then $n \leqslant m \wedge m \leqslant n \Rightarrow n = m$ and $n \neq m$ which is a contradiction. □

Theorem 5.50. *$\forall n, m \in \mathbb{N}_0$ with $n < m$ we have $s(n) \leqslant m$ [in other words using [theorem: 5.30] $n < m$ implies $n + 1 \leqslant m$].*

Proof. We proof this by induction, so given $n \in \mathbb{N}_0$, define $S_n = \{m \in \mathbb{N}_0 | n < m \Rightarrow s(n) \leqslant m\}$ then we have:

$0 \in S_n$. By [theorem: 5.49] $n < 0$ is false, so $n < 0 \Rightarrow s(n) \leqslant m$ is true, proving that $0 \in S_n$.

$m \in S_n \rightarrow s(m) \in S_n$. Let $n < s(m)$ then we have $n \neq s(m)$ and $n \leqslant s(m)$ so that $n \in s(m) = m \bigcup \{m\}$, hence we have to look at:

$n \in m$. By [theorem: 5.48] we have $n < m$, as $m \in S_n$ we have $s(n) \leqslant m$, as by [theorem: 5.47] $m < s(m)$ it follows by transitivity that $s(n) \leqslant s(m)$ [actually even $s(n) < s(m)$].

$n = m$. Then $s(n) = s(m)$ so that $s(n) \leqslant s(m)$.

So we have $s(m) \in S_n$

Using induction [theorem: 5.11] it follows that $\forall n, m \in \mathbb{N}_0$ with $n < m$ we have as $m \in S_n$ such that $s(n) \leqslant m$. □

Theorem 5.51. *$\langle \mathbb{N}_0, \leqslant \rangle$ is a well ordered set.*

Proof. We prove this by contradiction. Assume that there exist a A such that $\varnothing \neq A \subseteq \mathbb{N}_0$ with no least element. Define then

$$S_A = \{n \in \mathbb{N}_0 | \forall m \in A \text{ we have } n \leqslant m\}$$

then as A has no least element we must have that $S_A \bigcap A = \varnothing$ [for if $l \in S_A \bigcap A$ then $l \in A$ and $\forall m \in A$ we have $l \leqslant m$ so that l is a least elemet of A]. For S_A we have

$0 \in S_A$. If $m \in A$ we have by [theorem: 5.46] that $0 \leqslant m$ so that $0 \in S_A$.

$n \in S_A \Rightarrow s(n) \in S_A$. As $n \in S_A$ we have $\forall m \in A$ that $n \leqslant m,\ S_A \bigcap A = \varnothing$ so we have $n \neq m$ so that $n < m$, using then [theorem: 5.50] proves $s(n) \leqslant m$. Hence $s(n) \in S_A$

Using mathematicl induction we have $S_A = \mathbb{N}_0$, so that $S_A \bigcap A = \mathbb{N}_0 \bigcap A = A \neq \varnothing$ contradicting $S_A \bigcap A = \varnothing$. As the assumtion gives a contradiction every non empty subset of $\mathbb{N}_0$ has a least element and $\langle \mathbb{N}_0, \leqslant \rangle$ must be well ordered. □

As a consequence of the above we have:

Corollary 5.52. *$\langle \mathbb{N}_0, \leqslant \rangle$ is totally ordered and conditional complete.*

Proof. As $\langle \mathbb{N}_0, \leqslant \rangle$ is well ordered by [theorem: 5.51] we have by [theorem: 3.79] that $\langle \mathbb{N}_0, \leqslant \rangle$ is totally ordered and conditional complete. □

Corollary 5.53. *If $x, y \in \mathbb{N}_0$ then we have either $x \leqslant y$ or $y < x$*

Proof. As $\langle \mathbb{N}_0, \leqslant \rangle$ is well ordered the corollary follows from [theorem: 3.79]. □

Theorem 5.54. *$\forall n, m \in \mathbb{N}$ then $n < m \Leftrightarrow s(n) < s(m)$*

Proof.

$\Rightarrow$. From [theorem: 5.50] we have $s(n) \leqslant m$, as by [theorem: 5.47] $m < s(m)$ it follows that $s(n) < s(m)$.

$\Leftarrow$. Assume that $m \leqslant n$ then by [theorem: 5.47] we have $n < s(n)$ so that $n < s(m)$, using [theorem: 5.50] we have $s(n) \leqslant s(m)$, combining this with $s(n) < s(m) \Rightarrow s(n) \neq s(m) \wedge s(n) \leqslant s(m)$ gives the contradiction $s(n) = s(m) \wedge s(n) \neq s(m)$, so we have

$$\neg(m \leqslant n)$$

Using [corollary: 5.53] we have $m \leqslant n$ or $n < m$ so that we must have

$$n < m$$ □

Theorem 5.55. *If $n, m, k \in \mathbb{N}_0$ then we have*

$$n < m \Leftrightarrow n + k < m + k$$

which, using [theorem: 5.43], implies that

$$n \leqslant m \Leftrightarrow n + k \leqslant m + k$$

Proof. We use induction , so let $S = \{k \in \mathbb{N}_0 | \text{If } m, n \in \mathbb{N}_0 \text{ then } n < m \Leftrightarrow n + k < m + k\ \}$ then we have:

$0 \in S$. If $k = 0$ then for $n, m \in \mathbb{N}_0$ we have, as by [theorem: 5.29] $n = n + 0 \wedge m = m + 0$ that $n < m \Leftrightarrow n + 0 < m + 0$. So $0 \in S$.

$k \in S \Rightarrow s(k) \in S$. then we have

$$\begin{aligned} n < m & \underset{k \in S}{\Leftrightarrow} n + k < m + k \\ & \underset{[\text{theorem: } 5.50]}{\Leftrightarrow} s(n + k) < s(m + k) \\ & \underset{[\text{theorem: } 5.31}{\Leftrightarrow} n + s(k) < m + s(k) \end{aligned}$$

proving that $s(k) \in S$

Induction [theorem: 5.11] proves then $\mathbb{N}_0 = S$ completing the proof. □

Corollary 5.56. *If $n \in \mathbb{N}_0$ then we have:*

1. *If $k \in \mathbb{N}_0 \setminus \{0\}$ then $n < n + k$*

2. *If $k \in \mathbb{N}_0$ then $n \leqslant n + k$*

Proof.

1. If $k \neq 0$ then $0 < k$ so that by the above theorem [theorem: 5.55] we have
$$n \underset{\text{[theorem: 5.29]}}{=} 0 + n < n + k$$
2. As $0 \leqslant 0$ it follows from the above theorem [theorem: 5.55] we have that
$$n \underset{\text{[theorem: 5.29]}}{=} 0 + n \leqslant n + k$$ □

Theorem 5.57. *If $n, k \in \mathbb{N}_0$ then $n + k = 0$ implies $n = k = 0$.*

Proof. Suppose that $k \neq 0$ then as $0 \leqslant n \underset{\text{[theorem: 5.56]}}{\Rightarrow} 0 \leqslant n < n + k = 0$ so that $0 \neq 0$ a contradiction, so $k = 0$. But then $n = n + 0 = n + k = 0$. □

Theorem 5.58. *If $n, m \in \mathbb{N}_0$ with $n < s(m)$ then $n \leqslant m$.*

Note 5.59. As by [theorem: 5.30] $s(m) = m + 1$ this is equivalent with $n < m + 1 \Rightarrow n \leqslant m$

Proof. Using [corollary: 5.53] we have that either $n \leqslant m$ or $m < n$. If $m < n$ then by [theorem: 5.50] $s(m) \leqslant n$, which combined with the hypothesis $n < s(m)$ gives the contradiction $n < m$. Hence we must have $n \leqslant m$. □

Theorem 5.60. *If $n, m \in \mathbb{N}_0$ with $n < m$ then $\exists! k \in \mathbb{N}_0 \setminus \{0\}$ such that $m = n + k$.*

Proof. First we prove existance by induction, so let
$$S_n = \{m \in \mathbb{N}_0 | \text{If } n < m \text{ then there exist a } k \in \mathbb{N}_0 \text{ such that } k \neq 0 \text{ and } m = n + k\}$$
then we have:

$0 \in S_n$. As $n < 0$ is false by [theorem: 5.49], the condition is satisfied vacuously, proving that $0 \in S_n$.

$m \in S_n \Rightarrow s(m) \in S_n$. If $n < s(m)$ then we have by [theorem: 5.58] that $n \leqslant m$ so that we have the following possibilities to consider:

$n = m$. Then $n + 1 \underset{\text{[theorem: 5.30]}}{=} s(n) = s(m)$, as $1 = s(0) \neq 0$ we have if we take $k = 1$ that $k \neq 0$ and $n + k = s(m)$, proving that $s(m) \in S_n$

$n < m$. Then as $m \in S_n$ there exist a $l \in \mathbb{N}_0$ such that $l \neq 0$ and $n + l = m$. Now
$$s(m) = s(n + l) \underset{\text{[theorem: 5.31}}{=} n + s(l)$$
Take $k = s(l)$ then $n + k = s(m)$, further by [theorems: 5.46, 5.47] we have $0 \leqslant l \wedge l < s(l) = k$ so that $0 < k$ hence $k \neq 0$. This proves that in this case we also have $s(m) \in S_n$.

Induction [see theorem: 5.11] proves then that $\mathbb{N}_0 = S_n$. Hence if $n, m \in \mathbb{N}_0$ we have $m \in S_n$ so that if $n < m$ there exist a $k \in \mathbb{N}_0$ such that $k \neq 0$ and $m = n + k$.

Now for uniqueness assume that $n < m$ and there exists $k, l \in \mathbb{N}_0$ such that
$$k + n \underset{\text{[theorem: 5.33]}}{=} n + k = m = n + l \underset{\text{[theorem: 5.33]}}{=} l + n$$
then by [theorem: 5.43] $k = l$. □

Corollary 5.61. *If $n, m \in \mathbb{N}_0$ then $n < m \Leftrightarrow \exists! k \in \mathbb{N}_0 \setminus \{0\}$ such that $n + k = m$*

Proof.

$\Rightarrow$. This follows from the previous theorem [theorem: 5.60].

$\Leftarrow$. Let $k \in \mathbb{N}_0 \setminus \{0\}$ such that $n+k=m$. As $k \in \mathbb{N}_0 \setminus \{0\}$ we have $0<k$ so that by [theorem: 5.55] $0+n<k+n \underset{\text{[theorems: 5.29,5.33]}}{\Rightarrow} n<n+k=m$. □

Corollary 5.62. *If $n,m \in \mathbb{N}_0$ then $n \leqslant m \Leftrightarrow \exists! k \in \mathbb{N}_0$ such that $m=n+k$*

Proof.

$\Rightarrow$. If $n \leqslant m$ then we have either:

$n=m$. Then $m \underset{\text{[theorem: 5.29]}}{=} n+0$ where $0 \in \mathbb{N}_0$.

$n<m$. Then by the previous corollary [collary: 5.61] there exists a $k \in \mathbb{N}_0 \setminus \{0\} \subseteq \mathbb{N}_0$ such that $m=n+k$.

proving existence. For uniqueness anssume that $n+k=m=n+l$ then

$$k+n \underset{\text{[theorem: 5.33]}}{=} n+k=m=n+l \underset{\text{[theorem: 5.33]}}{=} l+n$$

proving by [theorem: 5.43] that $k=l$.

$\Leftarrow$. As $k \in \mathbb{N}_0$ we have either:

$k=0$. Then $m=n+0 \underset{\text{[theorem: 5.29]}}{=} n$ so that $n \leqslant m$.

$0<k$. Then by the previouss corollary [corollary: 5.61] we have $n<m$ so that $n \leqslant m$. □

The above corollary ensures that the following definition is well defined.

Definition 5.63. *If $n,m \in \mathbb{N}_0$ with $n \leqslant m$ then the **unique** $k \in \mathbb{N}_0$ such that $m=n+k$ is noted as $m-n$. So we have that $n+(m-n) \underset{\text{[theorem: 5.33]}}{=} (m-n)+n=m$ and using [theorem: 5.29] that $n-n=0$.*

Note 5.64. The condition $n \leqslant m$ is essential for the existance of $n-m$ as this is needed for [corollary: 5.62]. Later when we define the set $\mathbb{Z}$ of integers we will relax this condition.

Theorem 5.65. *If $n,m,k \in \mathbb{N}_0$ is such that $n \leqslant k$ then*

$$(k+m)-n=(k-n)+m=(m+k)-n$$

Proof. As $n \leqslant k$ we have by [theorem: 5.56] $n \leqslant k+m$ so that $(k+m)-n$ and $k-n$ are well defined. Now

$$\begin{aligned}((k-n)+m)+n &\underset{\text{[theorem: 5.32]}}{=} (k-n)+(m+n)\\ &\underset{\text{[theorem: 5.33}}{=} (k-n)+(n+m)\\ &\underset{\text{[theorem: 5.33]}}{=} ((k-n)+n)+m\\ &\underset{\text{defiition}}{=} k+m\end{aligned}$$

So we have that

$$(k+m)-n=(k-n)+m$$

Further using commutativity [theorem: 5.33] we have that $(m+k)-n=(k+m)-n$ so that

$$(m+k)-n=(k-n)+m$$

□

Theorem 5.66. *If $n,k \in \mathbb{N}_0$ then $(n+k)-n=k=(k+n)-n$*

Proof. As $n \leqslant n$ we can us the previous theorem [see theorem: 5.65] so that

$$(k+n)-n=(n+k)-n=(n-n)+k=0+k=k$$ □

Theorem 5.67. *Let $n,m \in \mathbb{N}_0$ such thet $n<m$ then $n \leqslant m-1$*

Proof. As $n<m$ we have by [theorem: 5.60] a $k\in\mathbb{N}_0\setminus\{0\}$ such that $m=n+k$. As $0\neq k$ we have by [theorem: 5.18] that there exist a $l\in\mathbb{N}_0$ such that $k=s(l)=l+1$, so $m=(n+l)+1$ which by [definition 5.63] means that $n+l=m-1$. Further by [theorem: 5.56] we have $n\leqslant n+l$ so that $n\leqslant m-1$. □

Theorem 5.68. *Let $n\in\mathbb{N}_0$ and $m\in\mathbb{N}_0\setminus\{0\}$ then $(m-1)\cdot n=n\cdot(m-1)=n\cdot m-n$*

Proof. As $0<m$ we have by [theorem: 5.50] that $1=s(0)\leqslant m$ so that $m-1$ is well defined. Now

$$n+(m-1)\cdot n\underset{\text{commutativity}}{=}(m-1)\cdot n+n=(m-1)\cdot n+1\cdot n=((m-1)+1)\cdot n=m\cdot n=n.m$$

so that $(m-1)\cdot n=n\cdot m-n$ and by commutativity [see theorem: 5.33] $n\cdot(m-1)=n\cdot m-n$ □

Theorem 5.69. *If $n,m,i\in\mathbb{N}_0$ then*

1. *If $n\leqslant i<m$ then $0\leqslant i-n<m-n$*
2. *If $n\leqslant i\leqslant m$ then $0\leqslant i-n\leqslant m-n$*

Proof.

1. As $n\leqslant i<m$ we have $n<m$. From [corollary: 5.53] it follows that $0\leqslant i-n\vee i-n<0$ and $i-n<m-n\vee m-n\leqslant i-n$. Now by [theorem: 5.49] we have that $i-n<0$ is false so we must have that $0\leqslant i-n$. If $m-n\leqslant i-n$ then by [theorem: 5.55] $m=(m-n)+n\leqslant(i-n)+n=n$ proving that $m\leqslant n$ which by [theorem: 5.49] contradicts with $n<m$, so we must have $i-n<m-n$.
2. As $n\leqslant i\leqslant m$ we have $n\leqslant m$. From [corollary: 5.53] it follows that $0\leqslant i-n\vee i-n<0$ and $i-n\leqslant m-n\vee m-n<i-n$. Now by [theorem: 5.49] we have that $i-n<0$ is false so we must have that $0\leqslant i-n$. If $m-n<i-n$ then by [theorem: 5.55] $m=(m-n)+n<(i-n)+n=n$ proving that $m<n$ which by [theorem: 5.49] contradicts with $n\leqslant m$, so we must have $i-n\leqslant m-n$. □

Theorem 5.70. *If $k,n,m\in\mathbb{N}_0$ such that $k\leqslant n\wedge k\leqslant m$ then we have*

$$n\leqslant m\Leftrightarrow n-k\leqslant m-k$$

Proof.

⇒. Using [theorem: 5.53] we have either $m-k<n-k$ or $n-k\leqslant m-k$, if $m-k<n-k$ we have by [theorem: 5.55] that $(m-k)+k<(n-k)+k$ so that $m<n$ which as $n\leqslant m$ gives the contradiction $m<m$, so we have $n-k\leqslant m-k$.

⇐. Using [theorem: 5.55] we have that $(n-k)+k\leqslant(m-k)+k$ so that $n\leqslant m$. □

Theorem 5.71. *If $n\in\mathbb{N}_0$ then there does not exist a $k\in\mathbb{N}_0$ such that $n<k<s(n)$*

Proof. Assume that $\exists k\in\mathbb{N}_0$ such that $n<k<s(n)$. As $n<k$ we have by [theorem: 5.50] that $s(n)\leqslant k$ which combined with $k<s(n)$ gives $s(n)<s(n)$ a contradiction. □

Theorem 5.72. *If $\varnothing\neq A\subseteq\mathbb{N}_0$ is a set such that $\sup(A)$ exist then $\sup(A)\in A$*

Proof. We have the following cases for $\sup(A)$ to consider:

$\sup(A)=0$. As $A\neq\varnothing$ there exist a $x\in A$, further as the $\sup(A)$ is a upper bound of A we have that $x\leqslant 0$, which by [theorem: 5.49] proves that $x=0=\sup(A)$, giving that $\sup(A)=x\in A$.

$\sup(A)\neq 0$. Using [theorem: 5.18] there exist a $k\in\mathbb{N}_0$ such that $s(k)=\sup(A)$. As $\langle\mathbb{N}_0,\leqslant\rangle$ is totally ordered [see theorem: 5.52] and $k<s(k)=\sup(A)$, it follows from the properties of the supremum [theorem: 3.67] that there exist a $a\in A$ such that $k<a\leqslant\sup(A)=s(k)$. As we can not have $k<a<s(k)$ [see theorem: 5.71], it follows that $a=\sup(A)$ so that $\sup(A)\in A$. □

Theorem 5.73. *If $n,m,r,s\in\mathbb{N}_0$ then*

1. *If $n<m\wedge r<s$ then $n+r<m+s$*
2. *If $n\leqslant m\wedge r\leqslant s$ then $n+r\leqslant m+r$*

3. *If* $n<m\wedge r\leqslant s$ *then* $n+r<m+r$
4. *If* $n\leqslant m\wedge r<s$ *then* $n+m<m+r$

Proof.

1. Using [theorem: 5.55] to follows that $n+r<m+r$ and $r+m<s+m \underset{\text{[theorem: 5.33]}}{\Rightarrow} n+r<m+s$ proving, using transitivity, that $n+r<m+1$.
2. Using [theorem: 5.55] to follows that $n+r\leqslant m+r$ and $r+m\leqslant s+m \underset{\text{[theorem: 5.33]}}{\Rightarrow} n+r\leqslant m+s$ proving, using transitivity, that $n+r<m+1$.
3. Using [theorem: 5.55] to follows that $n+r\leqslant m+r$ and $r+m<s+m \underset{\text{[theorem: 5.33]}}{\Rightarrow} n+r<m+s$ proving, using transitivity, that $n+r<m+1$.
4. Using [theorem: 5.55] to follows that $n+r<m+r$ and $r+m\leqslant s+m \underset{\text{[theorem: 5.33]}}{\Rightarrow} n+r<m+s$ proving, using transitivity, that $n+r<m+1$. □

Theorem 5.74. *Let* $n,m\in\mathbb{N}_0\backslash\{0\}$ *then* $n\cdot m\in\mathbb{N}_0\backslash\{0\}$.

Proof. As $m\neq 0$ it follows from [theorem: 5.18] that $\exists k\in\mathbb{N}_0$ such that $m=s(k)$. So $n\cdot m=n\cdot s(k) \underset{\text{[theorem: 5.38]}}{=} n+n\cdot k$. Further as $n\neq 0$ we have that $0<n$, so that by [theorem: 5.55] $n \underset{\text{[theorem: 5.29]}}{=} n+0\leqslant n+n\cdot k=n\cdot m$, using transitivity gives then finally $0<n\cdot m$. □

Theorem 5.75. *If* $n,m\in\mathbb{N}_0$ *such that* $n<m$ *then*

1. *If* $k\in\mathbb{N}_0\backslash\{0\}$ *then* $n\cdot k<m\cdot k$
2. *If* $k\in\mathbb{N}_0$ *then* $n\cdot k\leqslant m\cdot k$

Proof.

1. As $n<m$ we have by [theorem: 5.60] that there exist a $l\in\mathbb{N}_0\backslash\{0\}$ such that $m=n+l$. So

$$m\cdot k=(n+l)\cdot k \underset{\text{[theorem: 5.39]}}{=} n\cdot k+l\cdot k.$$

As $l,k\in\mathbb{N}_0\backslash\{0\}$ we have by [theorem: 5.74] that $l\cdot k\neq 0$ so that $0<l\cdot k$, hence using [theorem: 5.55] we have that

$$n\cdot k \underset{\text{[theorem: 5.29]}}{=} 0+n\cdot k<l\cdot k+n\cdot k \underset{\text{[theorem: 5.33]}}{=} n\cdot k+l\cdot k=m\cdot k$$

so that

$$n\cdot k<m\cdot k$$

2. If $k\in\mathbb{N}_0$ then we have either:

   $\boldsymbol{k=0}$. Then by [theorem: 5.36] we have $n\cdot k=0=m\cdot k$ so that $n\cdot k\leqslant m\cdot l$.

   $\boldsymbol{k\neq 0}$. Then by (1) $n\cdot k<m\cdot k\Rightarrow n\cdot k\leqslant m\cdot k$. □

Theorem 5.76. *If* $n,m\in\mathbb{N}_0$ *such that* $\exists k\in\mathbb{N}_0\backslash\{n\}$ *such that* $n\cdot k=m\cdot k$ *then* $n=m$.

Proof. Using [corollary: 5.53] we have that $n<m$, $m<n$ or $n=m$. If $n<m$ then by [theorem: 5.75] $n\cdot k<m\cdot k$ contradicting $n\cdot k=m\cdot k$, likewise if $m<n$ then by [theorem: 5.75] $m\cdot k<n\cdot k$ contradicting $n\cdot k=m\cdot k$. So we must have $n=m$. □

Theorem 5.77. (Archimedean Property) *If* $x,y\in\mathbb{N}_0$ *and* $x\neq 0$ *then there exists a* $z\in\mathbb{N}_0\backslash\{0\}$ *such that* $y<z\cdot x$

Proof. For y we have two possibilities:

$\boldsymbol{y=0}$. As $x\neq 0$ we have $y=0<x \underset{\text{[theorem: 5.37]}}{=} 1\cdot x$, so using $z=1$ proves the theorem.

$\boldsymbol{y\neq 0}$. Using [corollary: 5.53] we have for $x,y\in\mathbb{N}_0$ either:

$\boldsymbol{y\leqslant x}$. Then as $1<s(1)=2$ [see theorem: 5.47] we have $x \underset{\text{[theorem: 5.37]}}{=} 1\cdot x<2\cdot x$ [see: theorem: 5.75], hence $y<2\cdot x$, so using $z=2$ proves the theorem.

$\boldsymbol{x<y}$**.** Using [theorem: 5.60] there exist $k\in\mathbb{N}_0\backslash\{0\}$ such that

$$y=x+k \tag{5.14}$$

As $0<x$ we have by [theorem: 5.50] $1=s(0)\leqslant x$ so that by multiplication with k we have [see theorem: 5.75] that

$$k=1\cdot k\leqslant x\cdot k \tag{5.15}$$

As $0\neq k<s(k)$ and $x\neq 0$ we have by [see theorem: 5.75] that $k\cdot x<s(k)\cdot x\Rightarrow x\cdot k<x\cdot s(k)$ combining this with [eq: 5.15] gives that

$$k<x\cdot s(k) \tag{5.16}$$

Using [theorem: 5.55] we have

$$x+k=k+x<\cdot s(k)+x=x+x\cdot s(k)=x\cdot 1+x\cdot s(k)\underset{\text{distributivity}}{=}x\cdot(1+s(k))$$

or using [eq: 5.14] that $y<x\cdot(s+s(k))$. So if we take $z=1+s(k)$ we have that $y<x\cdot z$ which as also $0<1<1+s(k)$ proves the theorem. $\square$

Theorem 5.78. (Division) *If $m\in\mathbb{N}_0$ and $n\in\mathbb{N}_0\backslash\{0\}$ then there exists a* ***unique*** *$r\in\mathbb{N}_0$ and a unique $q\in\mathbb{N}_0$ such that*

$$m=n\cdot q+r \text{ and } 0\leqslant r<n$$

Proof. First we prove existence of q and r. As $n\in\mathbb{N}_0\backslash\{0\}$ $n\neq 0$ so that $0<n$. For m we have the following cases to consider:

$\boldsymbol{m=0}$**.** In this case taking $q=0$ and $r=0$ gives $n\cdot 0+0\underset{\text{[theorem: 5.36]}}{=}0+0\underset{\text{[theorem: 5.29]}}{=}0\cdot m+0$ and $0\leqslant 0<n$, so $q=0=r$ satisfies $m=n\cdot q+r$ and $0\leqslant r<n$.

$\boldsymbol{0<m}$**.** Then we have the following cases for n to consider:

$\boldsymbol{n=1}$**.** Take $q=m$ and $r=0$ then $n\cdot q+r=1\cdot m+0\underset{\text{[theorem: 5.29,5.37]}}{=}m$ and $0\leqslant 0<n$, so q,r satisfies $m=n\cdot q+r$ and $0\leqslant r<n$.

$\boldsymbol{n\neq 1}$**.** Then as $0<n\underset{\text{[theorem: 5.50]}}{\Rightarrow}1=s(0)\leqslant n$ we have $1<n$. By [theorem: 5.75] it follows that $m=1\cdot m<n\cdot m$, so if we define

$$A_{n,m}=\{x\in\mathbb{N}_0|m<n\cdot x\wedge x\leqslant m\}$$

then $m\in A_{n,m}$ proving that

$$A_{n,m}\neq\varnothing$$

As $\langle\mathbb{N}_0,\leqslant\rangle$ is well ordered [see theorem: 5.51] there exist a least element

$$q'=\min(A_{n,m})$$

If $q'=0$ then as $q'\in A_{n,m}$ we would have $m<n\cdot 0\underset{\text{[theroem: 5.36]}}{=}0$ a contraiction, hence we must have that $0<q'$. So by [theorem: 5.18] there exist a $q\in\mathbb{N}_0$ such that $s(q)=q'$. As $q<s(q)=q'$ [see theorem: 5.47] we must have that $q\notin A_{n,m}$, which, as $q<q'\leqslant m$, means that $n\cdot q\leqslant m$. From this we have by [theorem: 5.75] the existance of a $r\in\mathbb{N}_0$ such that

$$m=n\cdot q+r$$

Using [corollary: 5.53] w have either $n\leqslant r$ or $r<n$. If $n\leqslant r$ then by [theorem: 5.55] we have $n+n\cdot q\leqslant r+n\cdot q=n\cdot q+r=m$, hence

$$n\cdot q'=n\cdot s(q)\underset{\text{[theorem: 5.38}}{=}n+n\cdot q\leqslant m$$

As $q'\in A_{n,m}$ we have by definition that $m<n\cdot q'$ which combined with the above yields the contradiction $m<m$. So we must have

$$0\leqslant r<n$$

To summarize we have found q, r such that $m = n \cdot q + r$ and $0 \leqslant r < n$ proving existence.

Now to prove uniqueness. Assume that $n \cdot q + r = m = n \cdot q'' + r''$ and $0 \leqslant q < n$, $0 \leqslant q'' < n$ with $q \neq q''$ then by [corollary: 5.53] we have either $q < q''$, $q'' < q$ or $q = q'$. For the cases $q < q''$ or $q'' < q$ we have

$q < q''$. Then by [theorem: 5.50]

$$
\begin{aligned}
s(q) \leqslant q'' &\underset{\text{[theorem: 5.75}}{\Rightarrow} s(q) \cdot n \leqslant q'' \cdot n \\
&\underset{\text{[theroems 5.40]}}{\Rightarrow} n \cdot s(q) \leqslant q'' \cdot n \\
&\underset{\text{[theorem: 5.38]}}{\Rightarrow} n \cdot q + n \leqslant q'' \cdot n \\
&\underset{\text{[theorem: 5.55]}}{\Rightarrow} n \cdot q + n + r + r'' \leqslant q'' \cdot n + r + r'' \\
&\Rightarrow m + n + r'' \leqslant m + r \\
&\underset{\text{[theorem: 5.55]}}{\Rightarrow} n + r'' \leqslant r \\
&\underset{\text{[theorem: 5.56]}}{\Rightarrow} n \leqslant n + r'' \leqslant r
\end{aligned}
$$

contradicting $r < n$.

$q'' < q$. Then by [theorem: 5.50]

$$
\begin{aligned}
s(q'') \leqslant q &\underset{\text{[theorem: 5.75}}{\Rightarrow} s(q'') \cdot n \leqslant q \cdot n \\
&\underset{\text{[theroems 5.40]}}{\Rightarrow} n \cdot s(q'') \leqslant q \cdot n \\
&\underset{\text{[theorem: 5.38]}}{\Rightarrow} n \cdot q'' + n \leqslant q \cdot n \\
&\underset{\text{[theorem: 5.55]}}{\Rightarrow} n \cdot q'' + n + r + r'' \leqslant q \cdot n + r + r'' \\
&\Rightarrow m + n + r \leqslant m + r'' \\
&\underset{\text{[theorem: 5.55]}}{\Rightarrow} n + r \leqslant r'' \\
&\underset{\text{[theorem: 5.56]}}{\Rightarrow} n \leqslant n + r \leqslant r''
\end{aligned}
$$

contradicting $r < n$.

So we must have that $q = q''$ but then $r + n \cdot q = n \cdot q + r = m = n \cdot q + r'' = r'' + n \cdot q$ proving by [theorem: 5.55] that $r = r''$. ☐

5.5 Other forms of Mathematical Induction and Recursion

In this section we rewrite the theorem of induction and recursion using $n + 1$ instead of $s(n)$ [see theorem: 5.30]. First we introduce some definiions.

Definition 5.79. *Let $n \in \mathbb{N}_0$ then $\{n, \ldots \infty\}$ is defined as*

$$\{n, \ldots \infty\} = \{i \in \mathbb{N}_0 | n \leqslant i\}$$

Note 5.80. $\{0, \ldots, \infty\} = \{x \in \mathbb{N}_0 | 0 \leqslant x\} \underset{\text{[theorem: 5.46]}}{=} \mathbb{N}_0$

Definition 5.81. *Let $n, m \in \mathbb{N}_0$ then $\{n, \ldots, m\}$ is defined as*

$$\{n, \ldots, m\} = \{i \in \mathbb{N}_0 | n \leqslant i \wedge i \leqslant m\}$$

We have now the following variation on mathematical induction.

Theorem 5.82. (Mathematical Induction) *If $n \in \mathbb{N}_0$ and $X \subseteq \{n, \ldots, \infty\}$ is such that*

1. $n \in X$

2. *If* $i \in X$ *then* $i+1 \in X$

then $X = \{n, \ldots, \infty\}$*.*

Proof. Take $S = \{i \in \mathbb{N}_0 | i + n \in X\}$ then we have:

$\mathbf{0 \in S}$**.** As $0 + n \underset{\text{[theorem: 5.29]}}{=} n \in X$ we have $0 \in S$.

$\boldsymbol{i \in S \Rightarrow s(i) \in S}$**.** As $i \in S$ we have $i + n \in X$ so that by the hypothesis $(i + n) + 1 \in X$. Now

$$\begin{aligned}(i+n)+1 &\underset{\text{[theorem: 5.32]}}{=} i+(n+1)\\ &\underset{\text{[theorem: 5.33]}}{=} i+(1+n)\\ &\underset{\text{[theorem: 5.32]}}{=} (i+1)+n\\ &\underset{\text{[theorem: 5.30}}{=} s(i)+n\end{aligned}$$

so that $s(i) + n \in X$, proving $s(i) \in S$.

By mathematical induction we have that $S = \mathbb{N}_0$. If $i \in \{n, \ldots \infty\}$ then $n \leqslant i$ so by [theorem: 5.62] $\exists k \in \mathbb{N}_0$ such that $i = n + k \underset{\text{[theorem: 5.33]}}{=} k + n \underset{k \in \mathbb{N}_0 = S}{\Rightarrow} i \in X$. Hence $\{n, \ldots, \infty\} \subseteq X$ which together with $X \subseteq \{1, \ldots, n\}$ proves that

$$X = \{1, \ldots, \infty\}$$

□

For recursion we have the following theorems that follows from [theorem: 5.20], [theorem: 5.24] and [theorem: 5.26] by replacing $s(n)$ by its equivalent form $n + 1$.

Theorem 5.83. *Let* A *be a set,* $a \in A$ *and* $f: A \rightarrow A$ *a function then there exist a* ***unique*** *function*

$$\lambda: \mathbb{N}_0 \rightarrow A$$

such that:

1. $\lambda(0) = a$
2. $\forall n \in \mathbb{N}_0$ *we have* $\lambda(n+1) = f(\lambda(n))$

Further if $f: A \rightarrow A$ *is injective and* $a \notin f(A)$ *then* $\lambda: \mathbb{N}_0 \rightarrow A$ *is injective.*

Theorem 5.84. *Let* A *be a set,* $f: A \rightarrow A$ *a function then* $\forall n \in \mathbb{N}_0$ *there exist a* ***unique*** *function*

$$(f)^n: A \rightarrow A$$

such that:

1. $(f)^0 = \mathrm{Id}_A$
2. $(f)^{n+1} = f \circ (f)^n$

Theorem 5.85. *Let* A *be a set,* $a \in A$ *and* $g: \mathbb{N}_0 \times A \rightarrow A$ *then there exist a* ***unique*** *function*

$$\lambda: \mathbb{N}_0 \rightarrow A$$

such that:

1. $\lambda(0) = a$
2. $\forall n \in \mathbb{N}_0$ $\lambda(n+1) = g(n, \lambda(n))$

Corollary 5.86. *Let* A *be a set,* $a \in A$ *and* $g: \mathbb{N}_0 \times A \rightarrow A$ *then there exist a* ***unique*** *function*

$$\lambda: \mathbb{N}_0 \rightarrow A$$

such that:

1. $\lambda(0) = a$

2. $\forall n \in \{1, \ldots, \infty\}\ \lambda(n) = g(n-1, \lambda(n-1))$

Proof. Using [theorem: 5.85] there exists a $\lambda: \mathbb{N}_0 \to A$ such that

$$\lambda(0) = a \text{ and } \forall n \in \mathbb{N}_0\ \lambda(n+1) = g(n, \lambda(n)) \tag{5.17}$$

Let $n \in \{1,...,\infty\}$ then $1 \leqslant n$ so by [definition: 5.63] we have that $n-1 \in \mathbb{N}_0$ such that $n = (n-1)+1$, hence $\lambda(n) = \lambda((n-1)+1) = g(n-1, \lambda(n-1))$. □

In the above the function $\lambda: \mathbb{N}_0 \to A$ is specified by saying what $a \in A$ is and what the function $g: N_0 \times A \to A$ is. Ther exist a more intuitive way of specifying these requirement as is expressed in the following definitiosn.

Definition 5.87. *Let A be a set, $a \in A$ then we can define a function as follows:*

$$f: \mathbb{N}_0 \to A$$

is defined by:

1. $f(0) = a$
2. $f(n+1) = G(n, \lambda(n))$

where $G(n, \lambda(n))$ is a expression of two parameters. The above is equivalent with the function defined by [theorem: 5.85] where $a \in A$ and $g: \mathbb{N}_0 \times A \to A$ is defined by $g(n,x) = G(n,x)$.

Another way to define a recursive function is based on [corollary: 5.86]

Definition 5.88. *Let A be a set, $a \in A$ then we define $f: \mathbb{N}_0 \to A$ as follows*

$$f(n) = \begin{cases} a \textit{ if } n = 0 \\ G(n-1, f(n-1)) \textit{ if } n \in \{1, \ldots \infty\} \end{cases}$$

Which is equivalent with the function defined by [theorem: 5.86] where $a \in A$ and $g: \mathbb{N}_0 \times A \to A$ is defined by $g(n,x) = G(n,x)$.

Example 5.89. (Faculity) $\text{fac}: \mathbb{N}_0 \to \mathbb{N}_0$ is defined by

$$\text{fac}(n) = \begin{cases} 1 \text{ if n=0} \\ n \cdot \text{fac}(n-1) = ((n-1)+1) \cdot \text{fac}(n-1) \end{cases}$$

this is the function defined by [corollary: 5.86] where $a = 1$ and $g: \mathbb{N}_0 \times A \to A$ is define by $g(n, x) = (n+1) \cdot x$ then we have

$$\begin{array}{rcl} \text{fac}(0) & = & 1 \\ \text{fac}(1) & = & g(0, \text{fac}(0)) = (0+1) \cdot \text{fac}(0) = 1 \cdot \text{fac}(0) = 1 \cdot 1 = 1 \\ \text{fac}(2) & = & g(1, \text{fac}(1)) = (1+1) \cdot \text{fac}(1) = 2 \cdot \text{fac}(1) = 2 \cdot 1 = 2 \\ \text{fac}(3) & = & g(2, \text{fac}(2)) = (2+1) \cdot \text{fac}(2) = 3 \cdot \text{fac}(2) = 3 \cdot 2 = 6 \\ & \ldots & \\ \text{fac}(n) & = & g(n-1, \text{fac}(n-1)) = ((n-1)+1) \cdot \text{fac}(n-1) = n \cdot \text{fac}(n-1) \\ & \ldots & \end{array}$$

or in other words without using g

$$\begin{array}{rcl} \text{fac}(0) & = & 1 \\ \text{fac}(1) & = & 1 \cdot \text{fac}(0) = 1 \cdot 1 = 1 \\ \text{fac}(2) & = & 2 \cdot \text{fac}(1) = 2 \cdot 1 = 2 \\ \text{fac}(3) & = & 3 \cdot \text{fac}(2) = 3 \cdot 2 = 6 \\ & \ldots & \\ \text{fac}(n) & = & n \cdot \text{fac}(n-1) \\ & \ldots & \end{array}$$

which is exactly what we mean by the definition

$$\mathrm{fac}(n) = \begin{cases} 1 \text{ if n=0} \\ n \cdot \mathrm{fac}(n-1) \text{ if } n \in \{1, \ldots, \infty\} \end{cases}$$

Chapter 6

Finite and Infinite Sets

6.1 Equipotence

First we define the concept of equipotency which allows us to state that two sets have the same size without actually counting the number of eleemnts. The latter will turn out to be impossible for every set.

Definition 6.1. *Two sets A and B are **equipotent** if there exist a bijection $f: A \to B$. We note this as $A \approx B$.*

Theorem 6.2. *Let A, B, C be sets then*

1. $A \approx A$
2. *If $A \approx B$ then $B \approx A$*
3. *If $A \approx B \wedge B \approx C$ then $A \approx C$*

Proof.

1. $\mathrm{Id}: A \to A$ is a bijection [see example: 2.60] proving that $A \approx A$
2. As $A \approx B$ there existss a bijection $f: A \to B$ but then by [theorem: 2.67] $f^{-1}|B \to A|$ is also a bijection, so that $B \approx A$.
3. If $A \approx B$ and $B \approx C$ then there exists bijections $f: A \to B$ and $g: B \to C$, using [theorem: 2.69] we have that $g \circ f: A \to C$ is a bijection, so $A \approx C$. □

Next we define a relation that says one set is smaller or equal to another set.

Definition 6.3. *Let A, B be sets then $A \preccurlyeq B$ if there exist a $C \subseteq B$ such that $A \approx C$.*

The following relation expresses that one set is smaller then another set.

Definition 6.4. *Let A, B be sets then $A \prec B$ if $A \preccurlyeq B$ and $\neg(A \approx B)$*

Clearly we have the following:

Theorem 6.5. *If A is a set then $\mathcal{P}(A) \approx 2^A$*

Proof. As $2 = s(1) = s(s(0)) = s(\{\varnothing\}) = \{\varnothing\} \bigcup \{\{\varnothing\}\} = \{\varnothing, \{\varnothing\}\} = \{0, 1\}$ we have that $2^A = \{0, 1\}^A$, finally using [theorem: 2.71] there exist a bijection $\mathcal{P}(A)$ and $\{0, 1\}^A$. □

Theorem 6.6. *Let A, B be sets then $A \preccurlyeq B$ if and only if there exist a injection $f: A \to B$*

Proof.

⇒. If $A \preccurlyeq B$ then there exist a set $C \subseteq B$ and a bijection $f: A \to C$, as a bijection is injective we have that $f: A \to C$ is injective and finally by [theorem: 2.48] $f: A \to B$ is a injection.

$\Leftarrow$. If $f: A \rightarrow C$ is a injection then by [theorem: 2.62] $f: A \rightarrow f(A)$ is a bijection where $f(A) \subseteq B$ proving that $A \preccurlyeq B$. $\square$

Theorem 6.7. *If A is a set then there exist no surjection between A and $\mathcal{P}(A)$*

Proof. We prove this by contradiction. So assume that there exists a surjective function

$$f: A \rightarrow \mathcal{P}(A)$$

Define

$$B = \{x \in A | x \notin f(x)\}$$

As $B \subseteq A$ we have that $B \in \mathcal{P}(A)$ and by surjectivity there exists a $a \in A$ such that $f(a) = B$. If $a \in B$ then $a \notin f(a) = B$ leading to the contradiction $a \in B \wedge a \notin B$, so we must have $a \notin B = f(a)$ giving the contradiction $a \in B \wedge a \notin B$. So the the assumption must be wrong hence there is no surjection between A and $\mathcal{P}(A)$. $\square$

Corollary 6.8. *If A is a set then no subset of A can be equipotent with $\mathcal{P}(A)$ or 2^A*

Proof. First we prove that no subset of A can be equipotent with $\mathcal{P}(A)$. If $B \subseteq A$ then we have the following possible cases to consider:

***$B = A$*.** Then by [theorem: 6.7] we can not have a surjection between B and $\mathcal{P}(A)$, which as a bijection is surjection, proves that there is no bijection between B and $\mathcal{P}(A)$. So B is not equipotent with $\mathcal{P}(A)$.

***$B \subset A$*.** Then $A \setminus B \neq \varnothing$,$B \bigcap (A \setminus B) = \varnothing$ and $A = (A \setminus B) \bigcup B$. Assume now that B is equipotent with $\mathcal{P}(A)$ then a bijection $g: B \rightarrow \mathcal{P}(A)$ exist, take the constant function $C_\varnothing: A \setminus B \rightarrow \mathcal{P}(A)$ where $C_\varnothing(x) = \varnothing$ and form then using [theorem: 2.73] the function

$$f = g \bigcup C_\varnothing: A \rightarrow \mathcal{P}(A)$$

If $C \in \mathcal{P}(A)$ then, as g is bijective $\exists x \in B$ such that $(x, C) \in g \subseteq f$ or $f(x) = C$, hence f is a surjection which is not allowed by [theorem: 6.7]. So B is not equipotent with $\mathcal{P}(A)$.

If $B \approx 2^A$ then, as by [theorem: 6.5] $2^A \approx \mathcal{P}(A)$, we have by [theorem: 6.2]] that $B \approx \mathcal{P}(A)$ which we have just shown to be impossible. So B can not be equipotence with 2^A. $\square$

Theorem 6.9. *If A, B are sets, $A \neq \varnothing$ then there exists a injection $f: A \rightarrow B$ if and only there exist a surjection $g: B \rightarrow A$*

Proof.

$\Rightarrow$. Let $f: A \rightarrow B$ be a injection then by [theorem: 2.56] there exist a $g: B \rightarrow A$ such that $g \circ f = \mathrm{Id}_A$. If $x \in A$ then $y = \mathrm{Id}_A(y) = (g \circ f)(y) = g(f(y))$ so that g is surjective.

$\Leftarrow$. Let $g: B \rightarrow A$ be a surjection then by [theorem: 3.97] there exist a injective function f: $A \rightarrow B$. $\square$

Corollary 6.10. *If A, B are sets then $A \preccurlyeq B$ if and only if there exist a surjection $f: B \rightarrow A$*

Proof. This follows from [theorem: 6.6] and the above [theorem: 6.9]. $\square$

Theorem 6.11. *Let A, B, C, D classes with $A \bigcap C = \varnothing = B \bigcap D$, $A \approx B$ and $C \approx D$ then*

$$(A \bigcup C) \approx (B \bigcup D)$$

Proof. As $A \approx B$ and $C \approx D$ then there exists bijections $f: A \rightarrow B$ and $g: C \rightarrow D$ then by [theorem: 2.75] there exists a bijection $f \bigcup g: A \bigcup C \rightarrow B \bigcup D$. Hen ce $A \bigcup C \approx B \bigcup D$. $\square$

Theorem 6.12. *If A, B, C, D are sets such that $A \approx B$ and $C \approx D$ then $A \times C \approx B \times D$*

Proof. As $A \approx B$ and $C \approx D$ there exist bijections $f: A \rightarrow B$ and $g: C \rightarrow D$. Define

$$h: A \times C \rightarrow B \times D \text{ by } h(x, y) = (f(x), g(x))$$

then we have:

- **injectivity.** If $h(x, y) = h(x', y')$ then $(f(x), g(x)) = (f(x'), g(x'))$ so that $f(x) = f'(x)$ and $g(x) = g(x')$, as f and g are injective we have $x = x'$ and $y = y'$ so that $(x, y) = (x', y')$.
- **surjectivity.** If $(r, s) \in B \times D$ then as f, g are surjective there exists $x \in A$, $y \in C$ such that $r = f(x)$ and $s = g(y)$ so that $h(x, y) = (f(x), g(y)) = (r, s)$. □

Theorem 6.13. *If A, B, C, D are sets such that $A \approx B$ and $C \approx D$ then $A^C \approx B^D$*

Proof. As $A \approx B$ and $C \approx D$ then there exists bijections $f: A \rightarrow B$ and $g: D \rightarrow C$. If $x \in A^C$ then $x: C \rightarrow A$ is a function, so $x \circ g: D \rightarrow A$ is a function, hence $f \circ (x \circ g): D \rightarrow B$ is a function, proving that $f \circ (x \circ g) \in B^D$. Define now $h: A^C \rightarrow B^D$ by $h(x) = f \circ (x \circ g)$ then we have:

injectivity. If $x, y \in A^C$ satisfies $h(x) = h(y)$ then

$$\begin{array}{rcl} f \circ (x \circ g) = f \circ (y \circ g) & \Rightarrow & f^{-1} \circ (f \circ (x \circ g)) = f^{-1} \circ (f \circ (y \circ g)) \\ & \Rightarrow & (f^{-1} \circ f) \circ (x \circ g) = (f^{-1} \circ f) \circ (y \circ g) \\ & \Rightarrow & \mathrm{Id}_A \circ (x \circ g) = \mathrm{Id}_A \circ (y \circ g) \\ & \Rightarrow & x \circ g = y \circ g \\ & \Rightarrow & (x \circ g) \circ g^{-1} = (y \circ g) \circ g^{-1} \\ & \Rightarrow & x \circ (g \circ g^{-1}) = y \circ (g \circ g^{-1}) \\ & \Rightarrow & x \circ \mathrm{Id}_C = y \circ \mathrm{Id}_C \\ & \Rightarrow x = y & \end{array}$$

surjectivity. If $y \in B^D$ then $y: D \rightarrow B$ is a function so that $y \circ g^{-1}: C \rightarrow B$ is a function, hence $f^{-1} \circ (y \circ g^{-1}): C \rightarrow A$ is a function or $f^{-1} \circ (y \circ g^{-1}) \in A^C$. Further

$$\begin{array}{rcl} h(f^{-1} \circ (y \circ g^{-1})) & = & f \circ ((f^{-1} \circ (y \circ g^{-1})) \circ g) \\ & = & f \circ ((f^{-1} \circ y) \circ (g^{-1} \circ g)) \\ & = & f \circ ((f^{-1} \circ y) \circ \mathrm{Id}_D) \\ & = & f \circ (f^{-1} \circ y) \\ & = & (f \circ f^{-1}) \circ y \\ & = & \mathrm{Id}_B \circ y \\ & = & y \end{array}$$

□

Theorem 6.14. *If A, B are sets such that $A \approx B$ then $\mathcal{P}(A) \approx \mathcal{P}(B)$ and $2^A \approx 2^B$*

Proof. As $A \approx B$ and $2 \approx 2$ [see theorem: 6.2], we have by [theorem: 6.13] that $2^A \approx 2^B$. Further by [theorem: 6.8] $\mathcal{P}[A] \approx 2^A$ and $\mathcal{P}(B) \approx 2^B$, so by [theorem: 6.2] it follows that $\mathcal{P}(A) = \mathcal{P}(B)$. □

6.2 Finite, Infinite and Denumerable sets

6.2.1 Finite and Infinite sets

Applying the concept of initial segments [see definition: 3.44] on $\langle \mathbb{N}_0. \leqslant \rangle$ we have the following definition.

Definition 6.15. *Let $n \in \mathbb{N}_0$ then S_n is defined by*

$$S_n = \{m \in \mathbb{N}_0 | m < n\}$$

Actual we have already encountered the initial segments for $\langle \mathbb{N}_0, \leqslant \rangle$ because they are actual the natural numbers as is proved in the following theorem.

Theorem 6.16. *$\forall n \in \mathbb{N}_0$ we have $n = S_n$*

Proof. We prove this by induction. So let $S = \{n \in \mathbb{N}_0 | n = S_n\}$ then we have:

$0 \in S$. If $x \in S_0$ then $x < 0$ which by [theorem: 5.49] is false, so $S_0 = \varnothing = 0$ proving that $0 \in S$.

$n \in S \Rightarrow s(n) \in S$. As $n \in S$ we have that $n = S_n$ so that

$$s(n) = n \bigcup \{n\} = S_n \bigcup \{n\}$$

If $m \in s(n)$ then we have the following possibilities to consider:

$m = n$. Then by [theorem: 5.47] we have that $m < s(m) = s(n)$ so that $m \in S_{s(n)}$

$m \in S_n$. Then $m < n$ which as by [theorem: 5.47] $n < s(n)$ proves that $m < s(n)$ hence $m \in S_{s(n)}$

this proves that

$$s(n) \subseteq S_{s(n)} \tag{6.1}$$

If $m \in S_{s(n)}$ then $m < s(n)$, now by [theorem: 5.53] we have either $n < m$ or $m \leqslant n$. If $n < m$ then by [theorem: 5.50] we have $s(n) \leqslant m$ so that by transitivity we have $m < m$ a contradiction. So we must have that $m \leqslant n$, if $m = n$ then $m \in n \bigcup \{n\} = s(n)$ and if $m < n$ then $m \in S_n \subseteq S_n \bigcup \{n\} = s(n)$. So in all cases we have $m \in s(n)$ proving that $S_{s(n)} \subseteq s(n)$, combining this with [eq: 6.1] gives

$$s(n) = S_{s(n)}$$

proving that $s(n) \in S$.

Using induction [theorem: 5.11] it follows that $S = \mathbb{N}_0$ proving the theorem. □

Theorem 6.17. *Let $n, m \in \mathbb{N}_0$ then*

$$n \leqslant m \Leftrightarrow S_n \subseteq S_m.$$

In other words as $n = S_n$ and $m = S_m$ we have

$$n \leqslant m \Leftrightarrow n \subseteq m$$

Proof.

$\Rightarrow$. If $x \in S_n$ then $x < n$ which as $n \leqslant m$ proves that $x < m$ so that $x \in S_m$, hence $S_n \subseteq S_m$.

$\Leftarrow$. By definition if $n \leqslant m$ then either $n = m \underset{n = S_n, m = S_m}{\Rightarrow} S_n = S_m \Rightarrow S_n \subseteq S_m$ or $n \in m$ which by [theorem: 5.14] we have that $n \subseteq m \underset{n = S_n, m = S_m}{\Rightarrow} S_n \subseteq S_m$. □

Theorem 6.18. *Let $n, m \in \mathbb{N}_0$ with $n \leqslant m$ then*

$$\beta \colon \{n, \ldots, m\} \to S_{(m-n)+1} \text{ where } \beta(i) = i - n$$

is a bijection with inverse

$$\beta^{-1} \colon S_{(m-n)+1} \to \{n, \ldots, m\} \text{ where } \beta^{-1}(i) = i + n$$

Proof. We have for the function $\beta \colon \{n, \ldots, m\} \to S_{(m-n)+1}$ where $\beta(i) = i - n$ the following:

injectivity. If $k, l \in \{n, \ldots, m\}$ such that $\beta(k) = \beta(l)$ then $k - n = l - n$, so by [theorem: 5.43] $k = (k - n) + n = (l - n) + n = l$ proving that $k = l$.

surjectivity. If $k \in S_{(m-n)+1}$ then $0 \leqslant k < (m - n) + 1$ so that by [theorem: 5.58] $0 \leqslant k \leqslant m - n$, then by [theorem: 5.55] we have that $n = 0 + n \leqslant k + n \leqslant (m - n) + n = m$. If we take $i = k + n$ then we have $0 \leqslant i \leqslant m$ and further $i - n = (k + n) - n \underset{\text{[theroem: 5.66]}}{=} k$ proving that $\beta(i) = k$.

So $\beta: \{n, \ldots, m\} \rightarrow S_{(m-n)+1}$ is a bijection. Further we have if $k \in S_{(m-n)+1}$ that $k = \beta(\beta^{-1}(k)) = \beta^{-1}(k) - n$ so that by [theorem: 5.43] $k + n = (\beta^{-1}(k) - n) + n = \beta^{-1}(k)$ proving that

$$\beta^{-1}: S_{(m-n)+1} \rightarrow \{n, \ldots, m\} \text{ is defined by } \beta^{-1}(k) = k + n$$ □

We define now the concept of a finite set.

Definition 6.19. (Finite Set) *A set A is **finite** if $\exists n \in \mathbb{N}_0$ such that $n \approx A$*

Example 6.20. $\varnothing$ is finite.

Proof. $\varnothing: \varnothing \rightarrow \varnothing$ is a bijection by [example: 2.59], so as $0 = \varnothing$ we have that $0 \approx \varnothing$. □

Definition 6.21. (Infinite Set) *A set A is **infinite** if A is not **finite**.*

Definition 6.22. (Denumerable Set) *A set $A$is **denumerable** or **infinite countable** if*

$$\mathbb{N}_0 \approx A.$$

Definition 6.23. (Countable Set) *A set A is countable if it is **finite** or **denumerable.***

Theorem 6.24. *If A, B are sets such that $A \approx B$ then we have*

1. *If A is finite then B is finite*
2. *If A is denumerable then B is denumerable*
3. *If A is countable then B is countable.*

Proof.

1. As A is finite there exists a $n \in \mathbb{N}_0$ such that $n \approx A$ which as $A \approx B$ proves by [theorem: 6.2] that $n \approx B$ hence B is finite.
2. As A is denumerable $\mathbb{N}_0 \approx A$ which as $A \approx B$ proves by [theorem: 6.2] that $\mathbb{N}_0 \approx B$ hence B is finite.
3. As A is countable it is eaither finite or denumerable, (1) and (2) ensures then that B is either finite or denumerable. □

Lemma 6.25. *If A is a **denumerable** set and $a \in A$ then $A \setminus \{a\}$ is a denumerable set.*

Proof. As A is denumerable there exist a bijection $f: \mathbb{N}_0 \rightarrow A$. As $a \in A$ we have by surjectivity that $\exists n \in \mathbb{N}_0$ such that $f(n) = a$. Define now

$$g: \mathbb{N}_0 \rightarrow A \text{ where } g(i) = \begin{cases} f(i) \text{ if } i < n \\ f(i+1) \text{ if } n \leqslant i \end{cases}$$

which, as $\{x \in \mathbb{N}_0 | x < n\} \bigcap \{x \in \mathbb{N}_0 | n \leqslant x\} = \varnothing$ and $\mathbb{N}_0 = \{x \in \mathbb{N}_0 | x < n\} \bigcup \{x \in \mathbb{N}_0 | n \leqslant x\}$, is a function As for bijectivity we have:

injectivity. If $g(i) = g(i')$ then for i, i' we have either:

$\boldsymbol{i < n \wedge i' < n}$**.** Then $f(i) = g(i) = g(i') = f(i')$ which as f is injective proves that $i = i'$.

$\boldsymbol{i < n \wedge n \leqslant i'}$**.** Then $f(i) = g(i) = g(i') = f(i'+1)$ which as f is injective proves that $i = i'+1$, Now as $n \leqslant i' < i'+1 = i$ and $i < n$ we reach the contradiction $n < n$, so this case is not possible.

$\boldsymbol{n \leqslant i \wedge i' < n}$**.** Then $f(i+1) = g(i) = g(i') = f(i')$ which as f is injective proves that $i+1 = i'$. Now as $n \leqslant i < i+1 = i'$ and $i' < n$ we reach the contradiction $n < n$, so this case is not possible.

$\boldsymbol{n \leqslant i \wedge n \leqslant i'}$**.** Then $f(i+1) = g(i) = g(i') = f(i'+1)$, hence, as f is injective, we have $i+1 = i+1'$ or by [theorem: 5.43] $i = i'$.

So in all valid cases we have $i = i'$ proving injectivity.

surjectivity. If $y \in A \setminus \{x\}$ then there exists by surjectivity of f a $i \in \mathbb{N}_0$ such that $f(i) = y$. We can not have $i = n$, because we would then have $f(i) = f(n) = y \notin A \setminus \{y\}$. So we have either

$i < n$. Then $g(i) = f(i) = y$

$n < i$. Then by [theorem: 5.67] $n \leqslant i - 1$, so $g(i-1) = f((i-1)+1) = f(i) = y$

proving surjectivity. □

Lemma 6.26. *Let $n \in \mathbb{N}_0$ then n has no denumerable subset. In particular, as $n \subseteq n$, n is not denumerable.*

Proof. We prove this by induction, so define

$$S = \{n \in \mathbb{N}_0 | n \text{ does not contain a denumerable subset}\}$$

then we have:

$0 \in S$. As $0 = \varnothing$ we have if $A \subseteq 0$ that $A = \varnothing$. If now $\mathbb{N}_0 \approx A$ then there exists a bijection f: $\mathbb{N}_0 \to A$ so that $f(0) \in A = \varnothing$ which is a contradiction. So 0 does not contains a denumerable subset.

$n \in S \Rightarrow n + 1 \in S$. We proceed by contradiction, so assume that there exist a $A \subseteq n + 1 = s(n) = n \bigcup \{n\}$ which is denumerable. If $n \notin A$ then $A \subseteq n$ which is impossible because $n \in S$, so we must have that $n \in A$. Let $a \in A \setminus \{n\} \subseteq n \bigcup \{n\}$ then, as $a \neq n$, $a \in n$ proving that $A \setminus \{n\} \subseteq n$. Now by the previous lemma [lemma: 6.25] we have, as A is denumerable, that $A \setminus \{n\}$ is denumerable which is forbidden as $n \in S$. So the assumption is wrong, hence everys subset of $s(n)$ is not denumerable, proving that $n + 1 \in S$.

Using induction [see theorem: 5.82] it follows that $S = \{0, \ldots, \infty\} = \mathbb{N}_0$ proving the lemma. □

Theorem 6.27. *Let A be a set then A is infinite if and only if A contains a denumerable subset.*

Proof.

$\Rightarrow$. Let A be a infinite set. Using the well ordering theorem [see theorem: 3.121] there exists a order relation $\leqslant_A$ such that $\langle A, \leqslant_A \rangle$ is a well ordered set. Using [theorem: 3.91] and the fact that $\langle \mathbb{N}, \leqslant \rangle$ is well ordered [see theorem: 5.51] we have exactly one of the following cases:

$\langle \mathbb{N}_0, \leqslant \rangle$ is order isomorphic with $\langle A, \leqslant_A \rangle$. This implies that $A \approx \mathbb{N}_0$ so that A is a denumerable subset of itself.

$\langle \mathbb{N}_0, \leqslant \rangle$ is order isomorphic with an initial segment of $\langle A, \leqslant_A \rangle$. This implies that A has a denumerable subset [the initial segment].

$\langle A, \leqslant_A \rangle$ is order isomorphic with an initial segment of $\langle \mathbb{N}_0, \leqslant \rangle$. So there exists a $n \in \mathbb{N}_0$ such that $A \approx S_n \underset{\text{[theorem: 6.16]}}{=} n$ so that A is finite, contradicting the fact that A is infinite. Hence this case does not apply.

So in all applicable cases we have that A contains a denumerable subset.

$\Leftarrow$. Let $B \subseteq A$ be a denumerable subset of A. Assume that A is finite then there exists a $n \in \mathbb{N}_0$ such that $n \approx A$, hence there exist a bijection $f: A \to n$. As $B \subseteq A$ we have that $f_{|B}$: $B \to f(B)$ is a bijection [see theorems: 2.78, 2.62] so that $B \approx f(B)$, as B is denumerable $\mathbb{N}_0 \approx B$, so by [theorem: 6.2] it follows that $\mathbb{N}_0 \approx f(B) \subseteq n$. So there exists a denumerable subset of n which by [theorem: 6.26] is impossible. Hence A is not finite wich by definition means that A is infinite. □

Corollary 6.28. $\mathbb{N}_0$ *is infinite.*

Proof. As $\mathbb{N}_0 \approx \mathbb{N}_0$ $\mathbb{N}_0$ is denumerable, clearly $\mathbb{N}_0 \subseteq \mathbb{N}_0$ so by the previous theorem [theroem: 6.27] we have that $\mathbb{N}_0$ is infinite. □

Corollary 6.29. *Every set with a infinite subset is infinite.*

Proof. If A is a set such that there exists a infinite set B with $B \subseteq A$ then, as B is infinite, we have by [theorem: 6.27] the existence of a denumerable set $C \subseteq B$, but then $C \subseteq A$ and thus A has a denumerable subset. Using [theorem: 6.27] it follows that A is infinite. □

Corollary 6.30. *Every subset of a finite set is finite*

Proof. If a finite set would contain a infinite subset then by the previous theorem the finite set would be infinite. □

Theorem 6.31. *If A and B are finite sets then $A \bigcup B$ is a finite set.*

Proof. As A is finite we have by [theorem: 6.30] that $A \setminus B$ is finite. So there exists $n, m \in \mathbb{N}_0$ such that $n \approx A \setminus B$ and $m \approx B$, hence we have two bijections

$$f: A \setminus B \to n \underset{[\text{theorem: } 6.16]}{=} S_n \text{ and } g': B \to m \underset{[\text{theorem: } 6.16]}{=} S_m \tag{6.2}$$

Define

$$C = \{i \in \mathbb{N}_0 | n \leqslant i \wedge i < n + m\}$$

If $b \in B$ then $g'(b) \in S_n$, hence $0 \leqslant g'(b) < m$ so that by [theorem: 5.55] $n = 0 + n \leqslant g'(b) + n < m + n$ or $g'(b) + n \in C$. So

$$g: B \to C \text{ where } g(i) = g'(i) + n \tag{6.3}$$

defines a function. Further we have:

injectivity. If $g(b) = g(b')$ then $g'(b) + n = g'(b') + n$, so using [theorem: 5.43] $g'(b) = g'(b')$, hence, as g' is injective, we have $b = b'$.

surjectivity. If $i \in C$ then $n \leqslant i < n + m$, using [theorem: 5.60] there exist a $k \in \mathbb{N}_0$ such that $n + k = i$. If $m \leqslant k$ then by [theorem: 5.55] $n + m \leqslant n + k = i < n + m$ a contradiction. So $k < m$ and thus $k \in S_m$. As g' is surjective there exists a $b \in B$ such that $g'(b) = k$ and thus $g(b) = g'(b) = k + n = i$.

proving that

$$g: B \to C \text{ is a bijection} \tag{6.4}$$

Further if $i \in n \bigcap C = S_n \bigcap C$ then $i < n \wedge n \leqslant i$ yielding the contradiction $i < i$ so we have that

$$n \bigcap C \neq \varnothing \tag{6.5}$$

If $i \in n \bigcup C$ then either

***$i \in n$*.** Then, as $n = S_n$, we have $i < n$ which as $n \leqslant n + m$ proves that $i < n + m$ hence $i \in S_{n+m}$.

***$i \in C$*.** Then $i < n + m$ so that $i \in S_{n+m}$

proving

$$n \bigcup C \subseteq S_{n+m} \tag{6.6}$$

If $i \in S_{n+m}$ then $i < n + m$, further we have either $i < n$ so that $i \in S_n = n$ or $n \leqslant i$ giving $i \in C$, hence $i \in n \bigcup C$ or $S_{n+m} \subseteq n \bigcup C$ which by [eq: 6.6] proves that

$$n \bigcup C = S_{n+m} \tag{6.7}$$

Using [eq: 6.2], [eq: 6.4], [eq 6.5],[eq: 6.7], $A \bigcup B = (A \setminus B) \bigcup B$ and $(A \setminus B) \bigcap B = \varnothing$ allows use to use [theorem: 2.75] to get the bijection

$$f \bigcup g: A \bigcup B \to S_{n+m}$$

proving that

$$A \bigcup B \approx S_{n+m}$$

□

Lemma 6.32. *If $\{A_i\}_{i \in S_n}$ is such that $\forall i \in S_n$ A_i is finite then $\bigcup_{i \in S_n} A_i$ is finite.*

Proof. We use induction to prove this, so define

$$S = \left\{ n \in \mathbb{N}_0 | \text{If } \{A_i\}_{i \in S_n} \text{ satisfies } \forall i \in S_n \ A_i \text{ is finite then } \bigcup_{i \in S_n} A_i \text{ is finite} \right\}$$

then we have:

$0 \in S$. If $n = 0$ then $S_0 = 0 = \varnothing$ so that $\bigcup_{i \in S_0} A_i = \bigcup_{i \in \varnothing} A_i \underset{\text{[example: 2.104]}}{=} \varnothing$ which is finite, hence $0 \in S$.

$n \in S \Rightarrow n + 1 \in S$. Let $\{A_i\}_{i \in n+1}$ a family of finite sets. As $S_{n+1} = n + 1 = s(n) = n \bigcup \{n\} = S_n \bigcup \{n\}$ and $n \notin S_n$ we have that $S_{n+1} \setminus \{n\} = S_n$. So

$$\bigcup_{i \in S_{n+1}} A_i \underset{\text{[theorem: 2.117]}}{=} \left(\bigcup_{i \in S_{n+1} \setminus \{n\}} A_i \right) \bigcup A_n = \left(\bigcup_{i \in S_n} A_i \right) \bigcup A_n$$

As $n \in S$ we have that $\bigcup_{i \in S_n} A_i$ is finite which, as A_n is also finite, proves, using [theorem: 6.31] that $(\bigcup_{i \in S_n} A_i) \bigcup A_n$ is finite. So $\bigcup_{i \in S_{n+1}} A_i$ is finite proving that $n + 1 \in S$.

Mathematical induction [see theorem: 5.82] proves then the lemma. □

Theorem 6.33. *If $\{A_i\}_{i \in I}$ is a such that I is finite and $\forall i \in I$ A_i is finite then $\bigcup_{i \in I} A_i$ is finite.*

Proof. As I is finite there exists a $n \in \mathbb{N}_0$ and a bijection $f: S_n \to I$ so that by [theorem: 2.102] we have that

$$\bigcup_{i \in I} A_i = \bigcup_{i \in S_n} A_{f(i)} \tag{6.8}$$

Using the previous lemma [lemma: 6.32] it follows that $\bigcup_{i \in S_n} A_{f(i)}$ is finite, hence using [eq: 6.8] we have

$$\bigcup_{i \in I} A_i \text{ is finite}$$

□

Theorem 6.34. *A set A is infinite if and only if $\exists B \subset A$ such that $B \approx A$. In other words A is infinite if and only if A is equipotent with a proper subset of itself.*

Proof.

$\Rightarrow$. If A is infinite then by [theorem: 6.27] there exist a denumerable $B \subseteq A$. So there exists a bijection $f: \mathbb{N}_0 \to B$. Define now the function [taking in account that $(A \setminus B) \bigcap B = \varnothing$ and $A = (A \setminus B) \bigcup B)$]

$$g: A \to A \text{ where } g(x) = \begin{cases} x \text{ if } x \in A \setminus B \\ f(f^{-1}(x) + 1) \text{ if } x \in B \end{cases}$$

where $f^{-1}: B \to \mathbb{N}_0$ is the inverse of f.

Then we have:

$$g(A) = A \setminus \{f(0)\} \tag{6.9}$$

Proof. If $y \in g(A)$ then there exists a $x \in A$ such that $y = g(x)$, we have for x either:

$x \in A \setminus B$. Then $y = g(x) = x$ so that $y \in A \setminus B$ or as $f(0) \in B$ that $y \in A \setminus \{f(0)\}$.

$x \in B$. If $f(0) = f(f^{-1}(x) + 1)$ we have, as f is a bijection hence injective, that $0 = f^{-1}(x) + 1$ which contradicts $0 < f^{-1}(x) + 1$. So we must have that

$$f(0) \neq f(f^{-1}(x) + 1) = y.$$

proving $y \in A \setminus \{f(0)\}$.

So we conclude that

$$g(A) \subseteq A \setminus \{f(0)\} \tag{6.10}$$

If $y \in A \setminus \{f(0)\}$ then we have either:

$y \in B$. If $f^{-1}(y) = 0$ we would have that $y = f(f^{-1}(y)) = f(0)$ contradicting $y \in A \setminus \{f(0)\}$. So we have that $f^{-1}(y) \neq 0$ or $0 < f^{-1}(y)$, using [theorem: 5.67] we have then that $0 \leqslant f^{-1}(y) - 1$. Take then $x = f(f^{-1}(y) - 1) \in B \subseteq A$ then we have:

$$\begin{aligned} g(x) &= f(f^{-1}(x) + 1) \\ &= f(f^{-1}(f(f^{-1}(y) - 1)) + 1) \\ &= f((f^{-1}(y) - 1) + 1) \\ &= f(f^{-1}(y)) \\ &= y \end{aligned}$$

so that $y \in g(A)$.

$y \notin B$. Then $y \in A \setminus B$ so that $g(y) = y$ proving that $y \in g(A)$

So we conclude that $A \setminus \{f(0)\} \subseteq g(A)$ which combinined with [eq: 6.10] proves $g(A) = A \setminus \{f(0)\}$. □

Next we proof that $g: A \rightarrow A$ is injective

Proof. Let $x, x' \in A$ such that $g(x) = g(x')$ then for x, x' we have to consider the following possible cases:

$x \in B \wedge x' \in B$. then $f(f^{-1}(x) + 1) = g(x) = g(x') = f(f^{-1}(x') + 1)$ so that

$$\begin{aligned} f(f^{-1}(x) + 1) = f(f^{-1}(x') + 1) &\underset{f \text{ is injective}}{\Rightarrow} f^{-1}(x) + 1 = f^{-1}(x') + 1 \\ &\Rightarrow f^{-1}(x) = f^{-1}(x') \\ &\underset{f^{-1} \text{ is injective}}{\Rightarrow} x = x' \end{aligned}$$

$x \in B \wedge x' \notin B$. Then $f(f^{-1}(x) + 1) = g(x) = g(x') = x'$ so that $f(f^{-1}(x) + 1) \notin B$ contradicting $f: \mathbb{N}_0 \rightarrow B$. So this case does not apply.

$x \notin B \wedge x' \in B$. Then $x = g(x) = g(x') = f(f^{-1}(x) + 1)$ so that $f(f^{-1}(x) + 1) \notin B$ contradicting $f: \mathbb{N}_0 \rightarrow B$, So this case never occurs.

$x \notin B \wedge x' \notin B$. Then $x = g(x) = g(x') = x'$. □

So we have proved that

$$g: A \rightarrow A \text{ is injective} \tag{6.11}$$

Using [eq: 6.9] and [eq: 6.11] proves that $g: A \rightarrow A \setminus \{f(0)\}$ is a bijection or

$$A \approx A \setminus \{f(0)\}$$

Further as $f(0) \in B \subseteq A$ we have that $A \neq A \setminus \{f(0)\}$ giving $A \setminus \{f(0)\} \subset A$. Hence we have proved that A is equipotent with a proper subset of itself.

$\Leftarrow$. Assume that there exists a proper subset $B \subset A$ such that $A \approx B$ then there exists a bijection $f: A \rightarrow B$, resulting in the injection [see theorem: 2.48]

$$f: A \rightarrow A \text{ with } f(A) = B \subset A$$

As $f(A) \subset A$ there exists a $a \in A$ such that $a \notin f(A)$. Using recursion [theorem: 5.83] there exist a injection $\lambda: \mathbb{N}_0 \rightarrow A$ such that $\lambda(0) = a$ and $\forall n \in \mathbb{N}_0\ \lambda(n+1) = f(\lambda(n))$. Hence we have a bijection $\lambda: \mathbb{N}_0 \rightarrow \lambda(A)$ proving that $\lambda(A)$ is denumerable, as $\lambda(A) \subseteq A$ it follows from [theorem: 6.27] that A is infinite. □

The following theorem allows you to quantify the number of elements in a finite set.

Theorem 6.35. *If $n, m \in \mathbb{N}_0$ such that $n \approx m$ then $n = m$.*

Proof. Assume that $n \approx m$ then by [theorem: 5.53] we have either $n < m$, $m < n$ or $n = m$. If

$n < m$. Then $\forall i \in n = S_n$ we have $i < n < m \Rightarrow i < m$ so that $i \in S_m = m$ which as $n \neq m$ proves that $n \subset m$. So m is equipotent to a proper subset of itself which by [theorem: 6.34] would mean that m is infinite contradicting the fact that m is finite [as $m \approx m$].

$m < n$. Then $\forall i \in m = S_m$ we have $i < m < n \Rightarrow i < n$ so that $i \in S_n = n$ which as $n \neq m$ proves that $m \subset n$. So n is equipotent to a proper subset of itself which by [theorem: 6.34] would mean that n is infinite contradicting the fact that n is finite [as $n \approx n$].

So the only option left is

$$n = m$$ □

The previous theorem leads to the following observation: If A is a finite set then there exists a $n \in \mathbb{N}_0$ such that $n \approx A$, if there was also a $n' \in \mathbb{N}_0$ such that $n' \approx A$ then $n \approx n'$, hence $n = n'$. This leads to the following defintion.

Definition 6.36. *If A is a **finite** set then $\exists! n \in \mathbb{N}_0$ such that $n \approx A$. This unique number is noted as $\#A$, so $\#A \approx A$. $\#A$ can be interpreted as the number of elements in A.*

Theorem 6.37. *If A is a set then $A = \varnothing \Leftrightarrow \#A = 0$*

Proof.

$\Rightarrow$. If $A = \varnothing$ then by [example: 2.59] $\varnothing: \varnothing \to \oslash$ is a bijection, so as $0 = \varnothing$ we have $\#\varnothing = 0$.

$\Leftarrow$. If $\#A = 0$ then as $0 = \varnothing$ there exists a bijection $f: \varnothing \to A$, Assume that $A \neq \varnothing$ then there exist a $y \in A$ and as f is a bijection we would have a $x \in \varnothing$ such that $f(x) = y$ contradicting the fact that $\forall x\ x \notin \varnothing$. □

Theorem 6.38. *If A, B are finite sets then $A \times B$ is finite and $\#(A \times B) = \#A \cdot \#B$*

Proof. We have for A, B to consider the following possibilities:

$A = \varnothing \vee B = \varnothing$. Then $0 = \varnothing \approx A$ and $0 = \varnothing \approx B$ so that $\#A = 0 = \#B$, further by [theorem: 1.47] $0 = \varnothing = A \times B$ hence $\#(A \times B) = 0 = \#A \cdot \#B$.

$A \neq \varnothing \wedge B \neq \varnothing$. Take $n = \#A \neq 0$ and $m = \#B \neq 0$ then there exist bijections $f: B \to n = S_n$ and $g: A \to m = S_m$. Now $\forall x \in A$, $\forall y \in B$ we have $f(x) < n$ and $g(y) < m$, using [theorem: 5.67] we have $g(y) \leqslant m - 1$. So by [theorem: 5.75]

$$n \cdot g(x) = g(x) \cdot n \leqslant (m-1) \cdot n \underset{\text{[theorem: 5.68}}{=} m \cdot n - n,$$

further by [theorem: 5.73] we have

$$(m \cdot n - n) + f(x) < (m \cdot n - n) + n = m \cdot n = n \cdot m$$

This allows us to define the function

$$h: A \times B \to S_{n \cdot m} \text{ where } h(x, y) = n \cdot g(x) + f(x)$$

then we have:

injectivity. If $h(x, y) = h(x', y')$ then $n \cdot g(x) + f(x) = n \cdot g(x') + f(x')$. As $0 \leqslant f(x) < n$ and $0 \leqslant f(x') < n$ it follows from [theorem: 5.78] that $g(x) = g(x')$ and $f(x) = f(x')$ which as f, g are bijections gives $x = x'$ and $y = y'$ so that $(x, y) = (x', y')$.

surjectivity. If $z \in S_{n \cdot m}$ then $0 \leqslant z < n \cdot m$, using [theorem: 5.78] there exist a q, r such that $z = q \cdot n + r$ and $0 \leqslant r < n$. If $m \leqslant q \underset{\text{[theorem: 5.75]}}{\Rightarrow} m \cdot n \leqslant q \cdot n \underset{\text{[theorem: 5.55]}}{\Rightarrow} m \cdot n + r \leqslant q \cdot n + r = z < n \cdot m$ so that $n \cdot m + r < n \cdot m$ or $r + n \cdot m < 0 + n \cdot \underset{\text{[theorem: 5.55]}}{\Rightarrow} r < 0$ a contradiction, hence $q < m$. So we have proved that $r \in S_n$ and $q \in S_m$, as f, g are bijections there exists $x \in A$, $y \in B$ such that $f(x) = r$ and $g(y) = q$. So $h(x, y) = n \cdot g(x) + f(x) = n \cdot q + r = z$.

Hence we have $A \times B \approx S_{n \cdot m}$ proving that $A \times B$ is finite and $\#(A \times B) = n \cdot m = \#A \cdot \#B$. $\square$

Theorem 6.39. *If A, B are finite sets such that $A \bigcap B = \varnothing$ then $\#(A \bigcup B) = \#A + \#B$*

Proof. Let $n = \#A$, $m = \#B$ then there exist bijections $f: A \rightarrow S_n$ and $g: B \rightarrow S_m$. If $x \in A$ then $f(x) < n < n + m$ and if $x \in B$ then $g(x) < m \Rightarrow n + g(x) < n + m$, as further $A \bigcap B = \varnothing$ we can define the function

$$h: A \bigcup B \rightarrow S_{n+m} \text{ where } h(x) = \begin{cases} f(x) \text{ if } x \in A \\ n + g(x) \text{ if } x \in B \end{cases}$$

We prove now that this is a bijection.

injectivity. If $h(x) = h(x')$ then we have the following cases to consider for $x, x' \in A \bigcup B$:

$\boldsymbol{x \in A \wedge x' \in A}$**.** Then $f(x) = h(x) = h(x') = f(x')$ which as f is a bijection gives $x = x'$.

$\boldsymbol{x \in A \wedge x' \in B}$**.** Then $f(x) = h(x) = h(x') = n + g(x')$, now as $f(x) < n$ we have

$$n + g(x') = f(x) < n + 0$$

so that by [theorem: 5.55] $g(x') < 0$, a contradiction. So this case will never occur.

$\boldsymbol{x \in B \wedge x' \in A}$**.** Then $n + g(x) = h(x) = h(x') = f(x')$, now as $f(x') < n$ we have

$$n + g(x) = f'(x) < n + 0$$

so that by [theorem: 5.55] $g(x) < 0$, a contradiction. So this case will never occur.

$\boldsymbol{x \in B \wedge x \in B}$**.** Then $g(x) + n = n + g(x) = h(x) = h(x') = n + g(x') = g(x') + n$ so that by [theorem: 5.55] $g(x) = g(x')$, which as g is a bijection proves that $x = x'$.

surjectivity. If $y \in S_{n+m}$ then $y < n + m$ and we have the following cases for y to consider:

$\boldsymbol{y < n}$**.** Then $y \in S_n$ so that by surjectivity of f we have a $x \in A$ such that $f(x) = y$, hence $h(x) = f(x) = y$

$\boldsymbol{n \leqslant y}$**.** Then $n \leqslant y < n + m$, by [theorem: 5.69] we have then that $0 \leqslant y - m < (n + m) - n \underset{\text{[theorem: 5.66]}}{=} m$, proving that $y - n \in S_m$. As g is a surjection there exists a $x \in B$ such that $g(x) = y - n$, hence $h(n) = n + g(x) = n + (y - n) = y$. $\square$

Theorem 6.40. *If A is a finite set and $B \subseteq A$ then:*

1. *B is finite*
2. *$A \setminus B$ is finite*
3. *$\#B \leqslant \#A$*
4. *If $B \subset A$ then $\#B < \#A$*
5. *$\#A = \#B + \#(A \setminus B)$*

Proof. As A is finite there exist $n \in \mathbb{N}_0$ and a bijection $f: n = S_n \rightarrow A$. We have then to consider the following possibilities:

$\boldsymbol{B = A}$**.** Then obviously B is finite, $A \setminus B = \varnothing$ is also finite, $\#B = \#A \Rightarrow \#B \leqslant \#A$ and $\#B + \#(A \setminus B) = \#A + \#\varnothing \doteq \#A + 0 = \#A$, So (1), (2),(3), (4) and (5) are satisfied.

$\boldsymbol{B = \varnothing}$**.** Then clearly B is finite, $A \setminus B = A$ is finite, $\#B = 0 \leqslant \#A$ and $\#B + \#(A \setminus B) = 0 + \#A = \#A$, further if $B \subset A$ then $A \neq \varnothing$ so that $\#B = 0 < \#A$.

$\boldsymbol{\varnothing \neq B \subset A}$**.** As every subset of a finite set is finite [see theorem: 6.30] we have that B and $A \setminus B$ are finite, further as $B \subset A$ we have that $A \setminus B \neq \varnothing$ so that

$$0 < \#(A \setminus B).$$

As $B \bigcap (A \setminus B) = \varnothing$ and $A \bigcup B = (A \setminus B) \bigcup B$ it follows from [theorem: 6.39] that

$$\#A = \#B + \#(A \setminus B)$$

Now if $\#A\leqslant\#B$ then as $0<\#(A\setminus B)$ it follows from [theorem: 5.73] that

$$\#A=\#A+0<\#B+\#(A\setminus B)=\#A$$

a contradiction, so we must have that

$$\#B<\#A$$

So (1),(2),(3),(4) and (5) are satisfied. □

Corollary 6.41. *If A,B are sets, A is finite and $f:A\rightarrow B$ is a surjection then B is finite and $\#B\leqslant\#A$.*

Proof. If $B=\varnothing$ then B is finite and $\#B=0\leqslant\#A$ proving the theorem in this case. If $B\neq\varnothing$ then by [theorem: 6.9] there exist as injection $g:B\rightarrow A$, leading by [theorem: 2.62] to a bijection $g:B\rightarrow g(B)$, hence $B\approx g(B)$. As $g(B)\subseteq A$ we have by [theorem: 6.40] that $g(B)$ is finite and $\#g(B)\leqslant\#A$. Finally as $\#g(B)\approx B$ and $B\approx g(B)$ it follows that $\#B=\#g(B)\leqslant\#(A)$. □

Theorem 6.42. *Let I be a finite set and $\{x_i\}_{i\in I}\subseteq X$ a finite family of elements in X then $\{x_i|i\in I\}$ is finite.*

Proof. Define the function $f:I\rightarrow\{x_i|i\in I\}$ by $f(i)=x_i$ then if $y\in\{x_i|i\in I\}$ there exist a $i\in I$ such that $y=x_i$, hence $y=f(i)$. This proves that $f:I\rightarrow\{x_i|i\in I\}$ is a surjection, so by the previous corollary [corollary: 6.41] we have as I is finite that $\{x_i|i\in I\}$ is finite. □

Theorem 6.43. *Let A,B be sets, A infinite and $f:A\rightarrow B$ a injection then B is infinite.*

Proof. Assume that B is finite then $f(A)\subseteq B$ is finite and there is a bijection $g:n\rightarrow f(A)$, as $f:A\rightarrow f(A)$ is a bijection we have that $f^{-1}:f(A)\rightarrow A$ is a bijection so that $f^{-1}\circ g:n\rightarrow A$ is a bijection, hence A is finite, contradicting the fact that A is infinite. So the assumption is wrong hence B is infinite. □

Theorem 6.44. *Let $\langle X,\leqslant\rangle$ be a totally ordered set, $\varnothing\neq A\subseteq X$ a finite set then* $\max(A)$ *and* $\min(A)$ *exists.*

Proof. We prove this by induction on $\#A$, so let

$$S=\{n\in\{1,\ldots,\infty\}|\text{If } A\subseteq X \text{ with } \#A=n \text{ then} \max(A) \text{ and } \min(A) \text{ exists}\}$$

then we have:

$1\in S$. As $\#A=1=\{0\}$ there exists a bijection $f:\{0\}\rightarrow A$ so that $A=\{f(0)\}$ and $\max(A)=f(0)=\min(A)$.

$n\in S\Rightarrow n+1\in S$. Let $A\subseteq X$ with $\#A=n+1$ then $n+1=s(n)=n\bigcup\{n\}$, so that there exists a bijection $f:n\bigcup\{n\}\rightarrow A$. If $n\in n$ then $n<n$ a contradiction so we have $n\notin n$. Take now

$$f_{|n}:n\rightarrow A\setminus\{f(n)\}$$

then by [theorem: 2.78] $f_{|n}$ is injective. Further if $y\in A\setminus\{f(n)\}$ then, as f is a bijection, there exists a $i\in n+1$ such that $f(i)=y$, we can not have $i=n$ [because then $f(i)=f(n)$], so $i\neq n\Rightarrow i\in n$, proving that $f_{|n|}(i)=f(i)=y$. Hence $f_{|n}:n\rightarrow A$ is a surjection, which together with injectivity proving that

$$f_{|n}:n\rightarrow A\setminus\{f(n)\} \text{ is a bijection hence } \#(A\setminus\{f(n)\})=n$$

As $n\in S$ we have that $M=\max(A\setminus\{f(n)\})$ and $m=\min(A\setminus\{f(n)\})$ exists. We have now for $M,f(n)$ to consider the following possibilities::

$M\leqslant f(n)$. Then $\forall x\in A\setminus\{f(n)\}$ we have $x\leqslant M\leqslant f(n)\Rightarrow x\leqslant f(n)$ and for $x=f(n)$ $x\leqslant f(n)$. So $\forall x\in A$ we have $x\leqslant f(n)$, proving that $\max(A)$ exist and $\max(A)=f(n)$.

$f(n)<M$. Then $\forall x\in A$ we have $x\leqslant M$ so that $\max(A)$ exist and $\max(A)=M$

For $m, f(n)$ we need to consider:

$\boldsymbol{m \leqslant f(n)}$**.** Then $\forall x \in A$ we have $m \leqslant x$ so that $\min(A)$ exist and $\min(A) = m$.

$\boldsymbol{f(n) < m}$**.** Then $\forall x \in A \setminus \{f(n)\}$ we have $m \leqslant x$ so that $f(n) < m$ and for $x = f(n)$ $x \leqslant f(n)$. So $\forall x \in A$ we have $f(n) \leqslant x$ proving that $\min(A)$ exist and that $f(n) = \min(A)$.

As $\min(A)$ and $\max(A)$ exist it follows that $n+1 \in S$

Using induction [see theorem:5.82] it follows that $\{1, \ldots, \infty\} = S$. Assume now that $\varnothing \neq A \subseteq X$ such that A is finite we must have that $\#A \in \{1, \ldots, \infty\}$ [for if $\#A = 0$ then $A = \varnothing$], so that $\min(A)$ and $\max(A)$ exist. □

Theorem 6.45. *If A is a finite set and $f: \mathbb{N}_0 \rightarrow A$ a function then $\exists a \in A$ such that $f^{-1}(\{a\})$ is infinite.*

Proof. Assume that $\forall a \in A$ $f^{-1}(\{a\})$ is finite. As A is finite we have for the family $\{f^{-1}(\{a\})\}_{a \in A}$ by [theorem: 6.33] that $\bigcup_{a \in A} f^{-1}(\{a\})$ is finite. Now

$$\begin{aligned} x \in \bigcup_{a \in A} f^{-1}(\{a\}) &\Leftrightarrow \exists a \in A \text{ such that } x \in f^{-1}(\{a\}) \\ &\Leftrightarrow \exists a \in A \text{ such that } f(x) \in \{a\} \\ &\Leftrightarrow \exists a \in A \text{ such that } f(x) = a \\ &\Leftrightarrow x \in f^{-1}(A) \end{aligned}$$

So that $\mathbb{N}_0 = f^{-1}(A) = \bigcup_{a \in A} f^{-1}(\{a\})$ from which it follows that $\mathbb{N}_0$ is finite contradicting the fact that $\mathbb{N}_0$ is infinite [by theorem: 6.28]. So the assumption is wrong, hence $\exists a \in A$ such that $f^{-1}(\{a\})$ is infinite. □

Corollary 6.46. *If A is finite and $f: \mathbb{N}_0 \rightarrow A$ a function then $\exists a \in A$ such that $\forall n \in \mathbb{N}_0$ there exist a $m \in \{n, \ldots, \infty\}$ so that $f(m) = a$.*

Proof. By the preceding theorem [theorem: 6.45] there exist a $a \in A$ such that $f^{-1}(\{a\})$ is infinite. Assume now that $\exists n \in \mathbb{N}_0$ such that $\forall m \in \{n, \ldots, \infty\}$ we have $f(m) \neq a$. If $m \in f^{-1}(\{a\})$ then $f(m) \in \{a\} \Rightarrow f(m) = a$, so we must have that $m \notin \{n, \ldots, \infty\}$, hence $m < n$ or $m \in S_n$. So we have proved that $f^{-1}(\{a\}) \subseteq S_n$ a finite set, giving by [theorem: 6.40] that $f^{-1}(\{a\})$ is finite contradicting the fact that $f^{-1}(\{a\})$ is infinite. So the assumption must be wrong, hence $\forall n \in \mathbb{N}_0$ there exists a $m \in \{n, \ldots, \infty\}$ such that $f(m) = a$. □

6.2.2 Finite families

We show now that every finite family of elements of a totally ordered set can be sorted.

Theorem 6.47. *Let $\langle X, \leqslant \rangle$ be a totally ordered set, $n \in \mathbb{N}_0$ and $\{x_i\}_{i \in S_{n+1}} \subseteq X$ then there exists a bijection $\beta: S_{n+1} \rightarrow S_{n+1}$ such that $\forall i \in S_n$ we have $x_{\beta(i)} \leqslant x_{\beta(n)}$.*

Proof. We prove this by induction, so let

$$S = \{n \in \mathbb{N}_0 | \forall \{x_i\}_{i \in S_{n+1}} \subseteq X \text{ there exist a bijection } \beta: S_{n+1} \rightarrow S_{n+1} \text{ such that } \forall i \in S_n \; x_{\beta(i)} \leqslant x_{\beta(n)}\}$$

then we have:

$\boldsymbol{0 \in S}$**.** If $\{x_i\}_{i \in S_1 = \{0\}} \subseteq X$ then for the bijection $\beta = \mathrm{Id}_{S_1}: S_1 \rightarrow S_1$ we have $\forall i \in S_0 = \varnothing$ that $x_{\beta(i)} \leqslant x_{\beta(0)}$ is satisfied vacuously, proving that $0 \in S$.

$\boldsymbol{n \in S \Rightarrow n+1 \in S}$**.** Let $\{x_i\}_{i \in S_{(n+1)+1}} \subseteq X$ then for $\{x_i\}_{i \in S_{n+1}}$ we have, as $n \in S$, the existence of a bijection $\alpha: S_{n+1} \rightarrow S_{n+1}$ such that $\forall i \in S_n$ $x_{\alpha(i)} \leqslant x_{\alpha(n)}$. For x_{n+1} we have now two cases to consider:

$\boldsymbol{x_{\alpha(n)} \leqslant x_{n+1}}$**.** Define

$$\beta: S_{(n+1)+1} \rightarrow S_{(n+1)+1} \text{ by } \beta(i) = \begin{cases} \alpha(i) \text{ if } i \in S_{n+1} \\ n+1 \text{ if } i = n+1 \end{cases}$$

then we have:

injectivity. Let $i, j \in S_{(n+1)+1}$ be such that $\beta(i) = \beta(j)$ then we have the following possibilities:

$\boldsymbol{i \in S_{n+1} \wedge j \in S_{n+1}}$**.** Then $\alpha(i) = \beta(i) = \beta(j) = \alpha(j)$ which as α is a bijection proves that $i = j$.

$\boldsymbol{i \in S_{n+1} \wedge j = n+1}$**.** Then $\alpha(i) = \beta(i) = \beta(j) = n+1$ from which it follows that $n+1 = \alpha(i) \in S_{n+1}$ giving the contradiction $n+1$<n+1. So this case never occurs.

$\boldsymbol{i = n+1 \wedge j \in S_{n+1}}$**.** Then $n+1 = \beta(i) = \beta(j) = \alpha(j)$ from which it follows that $n+1 = \alpha(j) \in S_{n+1}$ giving the contradiction $n+1$<n+1. So this case never occurs.

$\boldsymbol{i = n+1 \wedge j = n+1}$**.** Then $i = j$

surjectivity. If $j \in S_{(n+1)+1}$ then we have the following possibilities:

$\boldsymbol{j = n+1}$**.** Then $n+1 = \beta(n+1)$.

$\boldsymbol{j \in S_n}$**.** Then as α is a bijection there exist a $i \in S_n$ such that $j = \alpha(i) \underset{i \in S_n}{\Rightarrow} j = \beta(i)$.

So $\beta: S_{(n+1)+1} \rightarrow S_{(n+1)+1}$ is a bijection. Let now $i \in S_{n+1}$ then we have the following possibilities:

$\boldsymbol{i = n}$**.** Then $x_{\beta(i)} = x_{\alpha(i)} = x_{\alpha(n)} \leqslant x_{n+1} = x_{\beta(n+1)}$.

$\boldsymbol{i \in S_n}$**.** Then $x_{\beta(i)} = x_{\alpha(i)} \leqslant x_{\alpha(n)} \leqslant x_{n+1} = x_{\beta(n+1)}$.

which proves that in this case we have $n+1 \in S$.

$\boldsymbol{x_{n+1} < x_{\alpha(n)}}$**.** Define

$$\beta: S_{(n+1)+1} \rightarrow S_{(n+1)+1} \text{ by } \beta(i) = \begin{cases} \alpha(i) \text{ if } i \in S_n \\ n+1 \text{ if } i = n \\ \alpha(n) \text{ if } i = n+1 \end{cases}$$

then we have:

injectivity. Let $i, j \in S_{(n+1)+1}$ such that $\beta(i) = \beta(j)$ then we have the following possibilities:

$\boldsymbol{i \in S_n \wedge j \in S_n}$**.** Then $\alpha(i) = \beta(i) = \beta(j) = \alpha(j)$ which as β is a bijection gives $i = j$.

$\boldsymbol{i \in S_n \wedge j = n}$**.** Then $\alpha(i) = \beta(i) = \beta(j) = n+1$ so that $n+1 = \alpha(i) \in S_{n+1}$ giving the contradiction $n+1 < n+1$, so this case never occurs.

$\boldsymbol{i \in S_n \wedge j = n+1}$**.** Then $\alpha(i) = \beta(i) = \beta(j) = \alpha(n)$, which as α is a bijection, gives $i = n$ contradicting $i \in S_n \Rightarrow i < n$, so this case never occurs.

$\boldsymbol{i = n \wedge j \in S_n}$**.** Then $n+1 = \beta(i) = \beta(j) = \alpha(j)$ so that $n+1 = \alpha(j) \in S_{n+1}$ giving the contradiction $n+1 < n+1$, so this case never occurs.

$\boldsymbol{i = n \wedge j = n}$**.** Then $i = j$.

$\boldsymbol{i = n \wedge j = n+1}$**.** Then $n+1 = \beta(i) = \beta(j) = \alpha(n)$ so that $n+1 = \alpha(n) \in S_{n+1}$ giving the contradiction $n+1 < n+1$, so this case never occurs.

$\boldsymbol{i = n+1 \wedge j \in S_n}$**.** Then $\alpha(n) = \beta(i) = \beta(j) = \alpha(j)$, which as α is a bijection gives $n = j \in S_n$ resulting in the contradiction $n < n$, so this case never occurs.

$\boldsymbol{i = n+1 \wedge j = n}$**.** Then $\alpha(n) = \beta(i) = \beta(j) = n+1$ so that $n+1 = \alpha(n) \in S_{n+1}$ leading to the contradiction $n+1 < n+1$, so this case never occur.

i = n+1 ∧ j = n+1. Then $i = j$.

surjectivity. Let $j \in S_{(n+1)+1}$ then we have the following possibilities to check:

j = n+1. then $\beta(n) = j$

j ∈ S_{n+1}. then as α is a bijection there exist a $i \in S_{n+1}$ so that $\alpha(i) = j$. If $i = n$ then $\beta(n+1) = \alpha(n) = j$ and if $i \in S_n$ then $\beta(i) = \alpha(i) = j$.

So $\beta: S_{(n+1)+1} \rightarrow S_{(n+1)+1}$ is a bijection. Let now $i \in S_{n+1}$ then we have to consider the following possibilities:

i = n. Then $x_{\beta(i)} = x_{n+1} \leqslant x_{\alpha(n)} = x_{\beta(n+1)}$.

i ∈ S_n. Then $x_{\beta(i)} = x_{\alpha(i)} \leqslant x_{\alpha(n)} = x_{\beta(n+1)}$,

which proves that in this case $n+1 \in S$.

Mathematical induction [seee theorem: 5.82] proves then that $S = \mathbb{N}_0$. □

Corollary 6.48. *Let $\langle X, \leqslant \rangle$, $n, m \in \mathbb{N}_0$ such that $n \leqslant m$ and $\{x_i\}_{i \in \{n, \ldots, m\}} \subseteq X$ then there exist a bijection $\alpha: \{n, \ldots, m\} \rightarrow \{n, \ldots, m\}$ such that $\forall i \in \{n, \ldots, m-1\}$ we have $x_{\alpha(i)} \leqslant x_{\alpha(m)}$*

Proof. Using [theorem: 6.18] there exists bijections

$$\beta: \{n, \ldots, m\} \rightarrow S_{(m-n)+1} \text{ where } \beta(i) = i - n \tag{6.12}$$

and

$$\beta^{-1}: S_{(m-n)+1} \rightarrow \{n, \ldots, m\} \text{ where } \beta(i) = i + n \tag{6.13}$$

Let $\{x_i\}_{i \in \{n, \ldots, m\}} \subseteq X$ then for $\{x_{\beta^{-1}(i)}\}_{i \in S_{(m-n)+1}}$ we have by [theorem: 6.47] a bijection

$$\gamma: S_{(m-n)+1} \rightarrow S_{(m-n)+1} \text{ such that } \forall i \in S_{m-n} \text{ we have } x_{\beta^{-1}(\gamma(i))} \leqslant x_{\beta^{-1}(\gamma(m-n))} \tag{6.14}$$

Define now the bijection

$$\alpha = \beta^{-1} \circ \gamma \circ \beta: \{n, \ldots, m\} \rightarrow \{n, \ldots, m\}$$

If $k \in \{n, \ldots, m-1\}$ then $n \leqslant k \leqslant m-1 < m$ so that by [theorem: 5.69] we have $0 \leqslant k - n < m - n$ or $0 \leqslant \beta(k) < m - n$. So $\beta(k) \in S_{m-n}$ and thus by [eq: 6.14] we have that

$$x_{\beta^{-1}(\gamma(\beta(k)))} \leqslant x_{\beta^{-1}(\gamma(m-n))} \underset{\beta(m)=m-n}{=} x_{\beta^{-1}(\gamma(\beta(m)))} \tag{6.15}$$

Hence

$$\begin{array}{rcl} x_{\alpha(k)} & = & x_{(\beta^{-1} \circ \gamma \circ \beta)(k)} \\ & = & x_{\beta^{-1}(\gamma(\beta(k)))} \\ & \leqslant_{[\text{eq: } 6.15]} & x_{\beta^{-1}(\gamma(\beta(m)))} \\ & = & x_{(\beta^{-1} \circ \gamma \circ \beta)(m)} \\ & = & x_{\alpha(m)} \end{array}$$

So we have found a bijection $\alpha: \{n, \ldots, m\} \rightarrow \{n, \ldots, m\}$ such that $\forall k \in \{n, \ldots, m-1\}$ $x_{\alpha(k)} \leqslant x_{\alpha(m)}$ □

Theorem 6.49. *Let $\langle X, \leqslant \rangle$ be a totally ordered set, $n \in \mathbb{N}_0$ and $\{x_i\}_{i \in S_{n+1}} \subseteq X$ then there exists a bijection $\beta: S_{n+1} \rightarrow S_{n+1}$ such that*

$$\forall i \in S_n \text{ we have } x_{\beta(i)} \leqslant x_{\beta(i+1)}$$

Proof. We proof this by induction, so let

$S = \{n \in \mathbb{N}_0 | \forall \{x_i\}_{i \in n+1} \subseteq X$ there exist a bijection $\beta: S_{n+1} \rightarrow S_{n+1}$ such that $\forall i \in S_n$ $x_{\beta(i)} \leqslant x_{\beta(i+1)}\}$

then we have:

0 ∈ *S*. Then $S_0 = \varnothing$ and $S_1 = \{0\}$. Let $\{x_i\}_{i \in S_1 = \{0\}} \subseteq X$ then, for the bijection $\beta: S_1 \rightarrow S_1$ where $\beta = \mathrm{Id}_{S_1}$, we have that, $\forall i \in S_0 = \varnothing$ $x_{\beta(i)} \leqslant x_{\beta(i+1)}$, is satisfied vacuously.

$n \in S \Rightarrow n+1 \in S$. Let $\{x_i\}_{i \in S_{(n+1)+1}} \subseteq X$ then by the previous theorem [theorem: 6.47] there exists a bijection

$$\alpha: S_{(n+1)+1} \to S_{(n+1)+1} \text{ such that } \forall i \in S_{n+1}\ x_{\alpha(i)} \leqslant x_{\alpha(n+1)} \tag{6.16}$$

Consider now $\{x_{\alpha(i)}\}_{i \in S_{n+1}}$ then as $n \in S$ we have the existance of a bijection

$$\gamma: S_{n+1} \to S_{n+1} \text{ such that } \forall i \in S_n \text{ we have } x_{\alpha(\gamma(i))} \leqslant x_{\alpha(\gamma(i+1))} \tag{6.17}$$

Define now

$$\beta: S_{(n+1)+1} \to S_{(n+1)+1} \text{ by } \beta(i) = \begin{cases} \alpha(\gamma(i)) \text{ if } i \in S_{n+1} \\ \alpha(n+1) \text{ if } i = n+1 \end{cases}$$

then we have:

injectivity. Let $k, l \in S$ be such that $\beta(k) = \beta(l)$ then we must consider the following possibilities:

$k \in S_{n+1} \wedge l \in S_{n+1}$. Then

$$(\alpha \circ \gamma)(k) = \alpha(\gamma(k)) = \beta(k) = \beta(l) = (\alpha(\gamma(l))) = (\alpha \circ \gamma)(l)$$

which as $\alpha \circ \lambda$ is a bijection proves that $k = l$.

$k \in S_{n+1} \wedge l = n+1$. Then $\alpha(n+1) = \beta(l) = \beta(k) = \alpha(\gamma(k))$ which, as α is a bijection, gives $n+1 = \gamma(k)$, as $\gamma(k) \in S_{n+1} \Rightarrow \gamma(k) < n+1$ we reach the contradiction $n+1 < n+1$, so this case never occurs.

$k = n+1 \wedge l \in S_{n+1}$. Then $\alpha(n+1) = \beta(k) = \beta(l) = \alpha(\gamma(l))$ which, as α is a bijection, gives $n+1 = \gamma(l)$, as $\gamma(l) \in S_{n+1} \Rightarrow \gamma(l) < n+1$, we reach the contradiction $n+1 < n+1$, so this case never occurs.

$k = n+1 \wedge l = n+1$. then $k = l$

surjectivity. If $k \in S_{(n+1)+1}$ we have, as α is a bijection, that there exist a $l \in S_{(n+1)+1}$ such that $\alpha(l) = k$, for l we have then the following possibilities:

$l = n+1$. Then $\beta(n+1) = \alpha(n+1) = k$

$l \in S_{n+1}$. Then as γ is a bijection there exist a $i \in S_{n+1}$ such that $l = \gamma(i)$, hence $\beta(i) = \alpha(\gamma(i)) = \alpha(l) = k$.

Further if $i \in S_{n+1}$ we have the following posibilities to consider:

$i = n$. Then $\gamma(n) \in S_{n+1}$ so that by [eq: 6.16] $x_{\alpha(\gamma(i))} \leqslant x_{\alpha(n+1)} = x_{\beta(n+1)}$ hence

$$x_{\beta(i)} = x_{\alpha(\gamma(i))} \leqslant x_{\beta(n+1)} = x_{\beta(i+1)}$$

$i \in S_n$. Then by [eq: 6.17] we have $x_{\alpha(\gamma(i))} \leqslant x_{\alpha(\gamma(i+1))}$ so that

$$x_{\beta(i)} = x_{\alpha(\gamma(i))} \leqslant x_{\alpha(\gamma(i+1))} = x_{\beta(i+1)}$$

Hence $\forall i \in S_{n+1}$ we have $x_{\beta(i)} \leqslant x_{\beta(i+1)}$ proving that $n+1 \in S$.

Mathematical induction [see theorem: 5.82] proves that $S = \mathbb{N}_0$ and thus the theorem. □

Corollary 6.50. *Let $\langle X, \leqslant \rangle$ be a totally ordered set, $n, m \in \mathbb{N}_0$ with $n \leqslant m$ and $\{x_i\}_{i \in \{n, \ldots, m\}} \subseteq X$ then there exist a bijection $\alpha: \{n, \ldots, m\} \to \{n, \ldots, m\}$ such that $\forall i \in \{n, \ldots, m-1\}\ x_{\alpha(i)} \leqslant x_{\alpha(i+1)}$*

Proof. Using [theorem: 6.18] there exists bijections

$$\beta: \{n, \ldots, m\} \to S_{(m-n)+1} \text{ where } \beta(i) = i - n \tag{6.18}$$

and

$$\beta^{-1}: S_{(m-n)+1} \to \{n, \ldots, m\} \text{ where } \beta(i) = i + n \tag{6.19}$$

Let $\{x_i\}_{i \in \{n, \ldots, m\}} \subseteq X$ then for $\{x_{\beta^{-1}(i)}\}_{i \in S_{(m-n)+1}}$ we have by [theorem: 6.49] a bijection

$$\gamma: S_{(m-n)+1} \to S_{(m-n)+1} \text{ such that } \forall i \in S_{m-n} \text{ we have } x_{\beta^{-1}(\gamma(i))} \leqslant x_{\beta^{-1}(\gamma(i+1))} \tag{6.20}$$

Define now the bijection

$$\alpha = \beta^{-1} \circ \gamma \circ \beta : \{n, \ldots, m\} \rightarrow \{n, \ldots, m\}$$

If $k \in \{n, \ldots, m-1\}$ then $n \leqslant k \leqslant m-1 < m$ so that by [theorem: 5.69] we have $0 \leqslant k - n < m - n$ or $0 \leqslant \beta(k) < m - n$. So $\beta(k) \in S_{m-n}$ and thus by [eq: 6.20] we have that

$$x_{\beta^{-1}(\gamma(\beta(k)))} \leqslant x_{\beta^{-1}(\gamma(\beta(k)+1))}$$

Now $\beta(k+1) = (k+1) - n \underset{[\text{theorem: } 5.65]}{=} (k-n) + 1 = \beta(k) + 1$ so that by the above we have

$$x_{\beta^{-1}(\gamma(\beta(k)))} \leqslant x_{\beta^{-1}\gamma(\beta(k+1))} \tag{6.21}$$

Hence

$$\begin{array}{rcl} x_{\alpha(k)} & = & x_{(\beta^{-1} \circ \gamma \circ \beta)(k)} \\ & = & x_{\beta^{-1}(\gamma(\beta(k)))} \\ & \leqslant_{[\text{eq: } 6.21]} & x_{\beta^{-1}(\gamma(\beta(k+1)))} \\ & = & x_{(\beta^{-1} \circ \gamma \circ \beta)(k+1)} \\ & = & x_{\alpha(k+1)} \end{array}$$

So we have found a bijection $\alpha: \{n, \ldots, m\} \rightarrow \{n, \ldots, m\}$ such that $\forall k \in \{n, \ldots, m-1\}$ $x_{\alpha(k)} \leqslant x_{\alpha(k+1)}$ $\square$

The next theorem allows use later to apply induction on the product of a finite family of sets.

Theorem 6.51. *Let $n \in \mathbb{N}_0$ and let $\{A_i\}_{i \in S_{n+1}}$ a family of sets then*

$$\prod_{i \in S_{n+1}} A_i \approx \left(\prod_{i \in S_n} A_i \right) \times A_n$$

Proof. If $x \in \prod_{i \in S_{n+1}} A_i$ then $x \in \left(\bigcup_{i \in S_{n+1}} A_i \right)^{S_{n+1}}$ such that $\forall i \in S_{n+1}$ we have $x(i) \in A_i$ or equivalently $x: S_{n+1} \rightarrow \bigcup_{i \in S_{n+1}} A_i$ is a function so that $\forall i \in S_{n+1}$ we have $x(i) \in A_i$. As $\forall i \in S_n$ we have $x(i) \in A_i \subseteq \bigcup_{i \in S_n} A_i$, it follows that $x_{|S_n}: S_n \rightarrow \bigcup_{i \in S_n} A_i$ is a function, so $x_{|S_n} \in \prod_{i \in S_n} A_i$. Hence we can define the following function

$$\beta: \left(\prod_{i \in S_{n+1}} A_i \right) \rightarrow \left(\prod_{i \in S_n} A_i \right) \times A_n \text{ by } \beta(x) \rightarrow (x_{|S_n}, x(n))$$

Then we have:

injectivity. If $\beta(x) = \beta(y)$ then $(x_{|S_n}, x(n)) = (y_{|S_n}, y(n))$ or $x_{|S_n} = y_{|S_n}$ and $x(n) = y(n)$. So if $i \in S_{n+1}$ we have either $i \in S_n$ then $x(i) = x_{|S_n}(i) = y_{|S_n}(i) = y(i)$ or $i = n$ and then $x(i) = x(n) = y(n) = y(i)$, proving that $x = y$.

surjectivity. Let $(y, a) \in (\prod_{i \in S_n} A_i) \times A_n$ then $y \in \prod_{i \in S_n} A_i$ and $a \in A_n$. Define then the function:

$$x: S_{n+1} \rightarrow \bigcup_{i \in S_{n+1}} A_i \text{ by } x(i) = \begin{cases} y(i) \text{ if } i \in S_n \\ a \text{ if } i = n \end{cases}$$

Then $\forall i \in S_{n+1}$ we have either $i \in S_n$ giving $x(i) = y(i) \in A_i$ or $i = n$ giving $x(i) = x(n) = a \in A_n$, proving that $x \in \prod_{i \in S_{n+1}} A_i$. Further as clearly $x_{|S_n} = y$ and $x(n) = a$ we have that $\beta(x) = y$. $\square$

We use the above theorem to prove that the product of a finite family of finite sets is finite.

Theorem 6.52. *Let $n \in \mathbb{N}_0 \setminus \{0\}$ and $\{A_i\}_{i \in S_n}$ be such that $\forall i \in S_n$ A_i is finite then $\prod_{i \in S_n} A_i$ is finite.*

Proof. we proof this by induction so define

$$S=\left\{n\in\{1,\ldots,\infty\}|\text{If }\{A_i\}_{i\in S_n}\text{satisifes }\forall i\in S_n\ \ A_i\text{ is finite then }\prod_{i\in S_n}A_i\text{ is finite}\right\}$$

then we have:

$1\in S$. Using [example: 2.120] there exist a bijection $\beta: A_0\rightarrow\prod_{i\in\{0\}}A_i$, hence as $S_1=\{0\}$ $A_0\approx\prod_{i\in S_1}A_i$. As A_0 is finite there exist a $k\in\mathbb{N}_0$ such that $k\approx A_0$ proving that $k\approx\prod_{i\in S_0}A_i$ or that $\prod_{i\in S_1}A_i$ is finite. So $1\in S$.

$n\in S$ then $n+1\in S$. Let $\{A_i\}_{i\in S_{n+1}}A_i$ be such that that $\forall i\in S_{n+1}$ we have that A_i is finite. As $n\in S$ we have that $\prod_{i\in S_n}A_i$ is finite so using [theorem: 6.38] it follows that $(\prod_{i\in S_n}A_i)\times A_n$ is finite. Hence $\exists k\in\mathbb{N}_0$ such that $k\approx(\prod_{i\in S_n}A_i)\times A_n$. Using [theorem: 6.51] we have $(\prod_{i\in S_n}A_i)\times A_n\approx\prod_{i\in S_{n+1}}A_i$ proving that $k\approx\prod_{i\in S_{n+1}}A_i$. Hence $\prod_{i\in S_{n+1}}A_i$ is finite proving that $n+1\in S$.

Using mathematical induction it follows that $S=\{1,\ldots,\infty\}$ proving the theorem. □

Corollary 6.53. *Let I be a non empty finite set and $\{A_i\}_{i\in I}$ is such that $\forall i\in I$ we have A_i is finite then $\prod_{i\in I}A_i$ is finite.*

Proof. As I is finite and $I\neq\varnothing$ there exists a $n\in\mathbb{N}_0\backslash\{0\}$ such that $k\approx I$, so there exist a bijection $f: S_k\rightarrow I$. Using [theorem: 2.125] we have that there exists a bijection $\beta: \prod_{i\in I}A_i\rightarrow\prod_{i\in S_k}A_{f(i)}$ hence $\prod_{i\in I}A_i\approx\prod_{i\in S_k}A_{f(i)}$. By [theorem: 6.52] we have that $\prod_{i\in S_k}A_{f(i)}$ is finite so there exists a $m\in\mathbb{N}_0$ such that $m\approx\prod_{i\in S_k}A_{f(i)}$, hence $m\approx\prod_{i\in I}A_i$, proving that $\prod_{i\in I}A_i$ is finite. □

6.2.3 Denumerable sets

Lemma 6.54. *Every subset of $\mathbb{N}_0$ is either finite or denumerable*

Proof. By [theorem: 5.51[$\langle\mathbb{N}_0,\leqslant\rangle$ is a well ordered set, hence by [theorem: 3.92] we have for $N\subseteq\mathbb{N}_0$ either:

1. N is order isomorph with $\mathbb{N}_0$ hence $N\approx\mathbb{N}_0$ proving that N is denumerable.
2. N is order isomorph with a initial segement of $\mathbb{N}_0$ so there exists a $n\in\mathbb{N}_0$ such that $N\approx S_n$ proving that N is finite. □

Theorem 6.55. *Every subset of a denumerable set is finite or denumerable.*

Proof. Let A be a denumerable set and $B\subseteq A$. As A is denumerable there exists a bijection

$$\beta: A\rightarrow\mathbb{N}_0$$

Using [theorem: 2.78] and [theorem: 2.62] we have that $\beta_{|B}: B\rightarrow\beta(B)$ is a bijection so that

$$\beta(B)\approx B$$

as $\beta(B)\subseteq\mathbb{N}$ we have by the previous lemma [lemma: 6.54] that either:

$\beta(B)\approx\mathbb{N}_0$. Then by [theorem: 6.2] $B\approx\mathbb{N}_0$ proving that B is denumerable.

$\beta(B)$ is finite. Then there exists a $n\in\mathbb{N}_0$ such that $\beta(B)\approx n$, by [theorem: 6.2] $B\approx n$ proving that B is finite. □

Theorem 6.56. $\mathbb{N}_0\times\mathbb{N}_0\approx\mathbb{N}_0$*, in other words* $\mathbb{N}_0\times\mathbb{N}_0$ *is denumerable/*

Proof. First define the function

$$f:\mathbb{N}_0\times\mathbb{N}_0\rightarrow\mathbb{N}_0\times\mathbb{N}_0\text{ where }f(k,m)=\left\{\begin{array}{l}(0,k+1)\text{ if m=0}\\(k+1,m-1)\text{ if }m\in\mathbb{N}_0\backslash\{0\}\end{array}\right.$$

If $f(k,m)=f(k',m')$ we have the following cases for m,m'

$\boldsymbol{m=0\wedge m'=0.}$ Then $m=m'$ and $(0,k+1)=f(k,m)=f(k',m')=(0,k'+1)$ so that $k+1=k'+1 \underset{[\text{theorem: } 5.43]}{\Rightarrow} k=k'$ hence $(k,m)=(k',m')$.

$\boldsymbol{m=0\wedge m'\in\mathbb{N}_0\setminus\{0\}.}$ Then $(0,k+1)=f(k,m)=f(k',m')=(k'+1,m'-1)$ so that $0=k'+1$ which as $0<s(k')=k'+1$ is a contradiction, so this case does not occur.

$\boldsymbol{m\in\mathbb{N}_0\setminus\{0\}\wedge m'=0.}$ Then $(k+1,m-1)=f(k,m)=f(k',m')=(0,k'+1)$ so that $0=k+1$ which as $<s(k)=k+1$ is a contradiction, so this case does not occur.

$\boldsymbol{m\in\mathbb{N}_0\setminus\{0\}\wedge m'\in\mathbb{N}_0\setminus\{0\}.}$ Then $(k+1,m-1)=f(k,m)=f(k',m')=(k'+1,m'-1)$ so that $k+1=k'+1 \underset{[\text{theorem: } 5.43]}{\Rightarrow} k=k'$ and $m-1=m'-1 \underset{[\text{theorem: } 5.43]}{\Rightarrow} m=(m-1)+1=(m'-1)+1=m'$ so that $(k,m)=(k',m')$

The above proves that

$$f:\mathbb{N}_0\times\mathbb{N}_0\rightarrow\mathbb{N}_0\times\mathbb{N}_0 \text{ is injective} \tag{6.22}$$

Assume that $f(k,m)=(0,0)$ then if $m=0$ we have $(0,0)=(0,k+1)$ giving the contradiction $0=k+1$ and if $m\neq 0$ we have $(k+1,m-1)$ giving the contradiction $0=k+1$. So the assumption is incorrect hence

$$(0,0)\notin f(\mathbb{N}_0\times\mathbb{N}_0) \tag{6.23}$$

Using [eq: 6.22] and [eq: 6.23] we can use recursion [see theorem: 5.83] to get a **injective** function

$$\lambda:\mathbb{N}_0\rightarrow\mathbb{N}_0\times\mathbb{N}_0 \text{ such that } \lambda(0)=(0,0) \text{ and } \forall n\in\mathbb{N}_0 \text{ we have } \lambda(n+1)=f(\lambda(n))$$

We prove now the following proposition about λ:

Proposition 6.57. *If there exist a $n,m\in\mathbb{N}_0$ such that $\lambda(n)=(0,m)$ then if $k,l\in\mathbb{N}_0$ is such that $k+l=m$ we have $\lambda(n+k)=(k,l)$.*

Proof. We proof this by induction so let

$$S_{n,m}=\{k\in\mathbb{N}_0|\text{For } l\in\mathbb{N}_0 \text{ with } k+l=m \text{ we have } \lambda(n+k)=(k,l)\}$$

then we have:

$\boldsymbol{0\in S_{n,m}.}$ If $l\in\mathbb{N}_0$ such that $k+l=m$ then $l=m$ and $\lambda(n+k)=\lambda(n)=(0,m) \underset{k=0\wedge l=m}{=} (k,l)$ proving that $0\in S_{n,m}$.

$\boldsymbol{k\in S_{n,m}\Rightarrow k+1\in S_{n,m}.}$ If $l\in\mathbb{N}_0$ such that $(k+1)+l=m$ then we have $k+(l+1)=m$ and as $k\in S_{n,m}$ it follows that

$$\lambda(n+k)=(k,l+1) \tag{6.24}$$

Further

$$\begin{array}{rcl} \lambda(n+(k+1)) & = & \lambda((n+k)+1)\\ & = & f(\lambda(n+k))\\ & \underset{[\text{eq: } 6.24]}{=} & f(k,l+1)\\ & \underset{l+1\neq 0}{=} & (k+1,(l+1)-1)\\ & \underset{[\text{theorem: } 5.66]}{=} & (k+1,l) \end{array}$$

proving that $k+1\in S_{n,m}$.

Using induction [theorem: 5.82] it follows that $S_{n,m}=\mathbb{N}_0$ proving the proposition. □

We prove now using induction that $\lambda:\mathbb{N}_0\rightarrow\mathbb{N}_0\times\mathbb{N}_0$ is surjective. So let

$$S=\{n\in\mathbb{N}_0|\text{For } (k,m)\in\mathbb{N}_0\times\mathbb{N}_0 \text{ with } k+m=n \text{ there exists a } l\in\mathbb{N}_0 \text{ such that } \lambda(l)=(k,m)\}$$

$\boldsymbol{0\in S.}$ If $(k,m)\in\mathbb{N}_0\times\mathbb{N}_0$ is such that $k+m=0$ then we must have $k=m=0$, as $\lambda(0)=(0,0)=(k,l)$ we have $0\in S$.

$n \in S$ then $n+1 \in S$. Let $(k,m) \in \mathbb{N}_0$ be such that $k+m=n+1$, then for k we have to consider the following cases:

$k=0$. Then $m=k+m=n+1$ so that $(k,m)=(0,m)=(0,n+1)=f(n,0)$. As $n \in S$ and $n=n+0$ there exist a $l \in \mathbb{N}_0$ such that $\lambda(l)=(n,0)$. So

$$\lambda(l+1)=f(\lambda(l))=f(n,0)=(0,n+1)\underset{k=0}{=}(k,m)$$

$k \neq 0$. Then $0<k$ so that $0 \leqslant k-1$, further as $0 \neq m+1$ we have that

$$f(k-1,m+1)=((k-1)+1,(m+1)-1)=(k,m)$$

Let $k'=(k+m)-1 \underset{\mathrm{k+m=n+1}}{=} (n+1)-1=n$ and $l'=0$ then $k'+l'=n$ so that, as $n \in S$, there exist a $l \in \mathbb{N}_0$ such that

$$\lambda(l)=(k',l')=((k+m)-1,0) \tag{6.25}$$

Hence

$$\begin{array}{rcl}\lambda(l+1) & = & f(\lambda(l))\\ & \underset{\text{[eq: 6.25]}}{=} & f((k+m)-1,0)\\ & = & (0,k+m)\end{array}$$

Combining the above with [proposition: 6.57] we have that $\lambda((l+1)+k)=(k,m)$, so that $n+1 \in S$.

By mathematical induction [theorem: 5.82] it follows that $S=\mathbb{N}_0$. So if $(k,m) \in \mathbb{N}_0 \times \mathbb{N}_0$ we have that $k+m \in \mathbb{N}_0 = S$ so that $\exists n \in \mathbb{N}_0\ \lambda(n)=(k,m)$ which proves that λ is a surjection. Hence as λ is also injective it follows that $\lambda: \mathbb{N}_0 \rightarrow \mathbb{N}_0 \times \mathbb{N}_0$ is a bijection, proving that $\mathbb{N}_0 \times \mathbb{N}_0$ is denumerable. □

Corollary 6.58. *If A,B are denumerable then $A \times B$ is denumerable*

Proof. As A,B are denumerable we have $\mathbb{N}_0 \approx A$ and $\mathbb{N}_0 \approx B$, proving by [theorem: 6.12] that $\mathbb{N}_0 \times \mathbb{N}_0 \approx A \times B$. Finally as $\mathbb{N}_0 \approx \mathbb{N}_0 \times \mathbb{N}_0$ it follows that that $\mathbb{N}_0 \approx A \times B$. □

Corollary 6.59. *If $n \in \mathbb{N}_0 \backslash \{0\}$ then $n \times \mathbb{N}_0$ is denumerable*

Proof. As $n=S_n \subseteq \mathbb{N}_0$ we have by [theorem: 1.48] that $n \times \mathbb{N}_0 \subseteq \mathbb{N}_0 \times \mathbb{N}_0$ so that by [theorem: 6.55]

$$n \times \mathbb{N}_0 \text{ is either finite or denumerable}$$

As $n \neq 0$ we have that $n \neq \varnothing$ so there exist a $m \in n$, define then

$$\beta: \mathbb{N}_0 \rightarrow \{m\} \times \mathbb{N}_0 \text{ by } \beta(i)=(m,i)$$

then we have:

injectivity. If $\beta(i)=\beta(i')$ then $(m,i)=(m,i')$ giving $i=i'$

surjectivity. If $(x,y) \in \{m\} \times \mathbb{N}_0$ then $x=m$ and $y \in \mathbb{N}_0$ so that $\beta(y)=(m,y)=(x,y)$

So $\beta: \mathbb{N}_0 \rightarrow \{m\} \times \mathbb{N}_0$ is a bijection proving that $\{m\} \times \mathbb{N}_0$ is denumerable. As $\{m\} \times \mathbb{N}_0 \subseteq n \times \mathbb{N}_0$ it follows by [theorem: 6.27] that $n \times \mathbb{N}_0$ is not finite so $n \times \mathbb{N}_0$ must be denumerable. □

Corollary 6.60. *If A is a non empty finite set and B a denumerable set then $A \times B$ and $B \times A$ are denumerable sets.*

Proof. As $A \neq \varnothing$ and finite there exist a $n \notin \mathbb{N}_0 \backslash \{0\}$ such that $n \approx A$, as B is denumerable $\mathbb{N}_0 \times B$ we have by [theorem: 6.12] that

$$n \times \mathbb{N}_0 \approx A \times B$$

which as $\mathbb{N}_0 \approx \mathbb{N}_0 \times \mathbb{N}_0$ [see corollary: 6.59] proves that $\mathbb{N}_0 \approx A \times B$, hence

$$A \times B \text{ is denumerable}$$

Define the function

$$\beta: A \times B \rightarrow B \times A \text{ by } \beta(x, y) = (y, x)$$

then we have

injectivity. If $\beta(x, y) = \beta(x', y')$ then $(y, x) = \beta(x, y) = \beta(x', y') = (y', x')$ so that $x = x' \wedge y = y'$ proving that $(x, y) = (x', y')$.

surjectivity. If $(x, y) \in B \times A$ we have that $(y, x) \in A \times B$ so that $\beta(y, x) = (x, y)$.

proving that

$$\beta: A \times B \rightarrow B \times A \text{ is a bijection}$$

hence $A \times B \approx B \times A$, which as $A \times B \approx \mathbb{N}_0$ proves that

$$B \times A \text{ is denumerable.}$$

□

Theorem 6.61. *If $\{A_i\}_{i \in I}$ is such that $I \neq \varnothing \wedge I$ is finite and $\forall i \in I$ A_i is denumerable then $\bigcup_{i \in I} A_i$ is denumerable. In other words the union of a finite family of denumerable sets is denumerable.*

Proof. As I is finite and non empty there exist $n_0 \in \mathbb{N}_0 \setminus \{0\}$ and a bijection $\beta: n_0 \rightarrow I$. Further as $\forall i \in I$ A_i is denumerable there exist a bijection $\alpha_i: \mathbb{N}_0 \rightarrow A_i$. Define now the function

$$g: n_0 \times \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ by } g(n, m) = \alpha_{\beta(n)}(m)$$

Now if $y \in \bigcup_{i \in I} A_i$ there exist a $l \in I$ such that $y \in A_l$, as β is bijective there exists a $n \in n_0$ such that $\beta(n) = l$. As $\alpha_l: \mathbb{N}_0 \rightarrow A_l$ is a bijection there exist a $m \in \mathbb{N}_0$ such that $\alpha_l(m) = y$. So

$$g(n, m) = \alpha_{\beta(n)}(m) = \alpha_l(m) = y$$

proving that

$$g: n_0 \times \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ is surjective}$$

Now by [theorem: 6.59] there exist a bijection $\gamma: \mathbb{N}_0 \rightarrow n_0 \times \mathbb{N}_0$ so that

$$g \circ \gamma: \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ is surjective}$$

Using [theorem: 6.10] we have that $\bigcup_{i \in I} A_i \preccurlyeq \mathbb{N}_0$ which by [definition: 6.3] gives that $\exists E \subseteq \mathbb{N}_0$ such that $\bigcup_{i \in I} A_i \approx E$. Using [theorem: 6.55] we have that E is either finite or E is denumerable so that $\bigcup_{i \in I} A_i$ is either finite or denumerable. As $n_0 \neq 0 \Rightarrow 0 < n_0$ we have $0 \in S_{n_0} = n_0$, so that $\beta(0) \in I$, hence $A_{\beta(0)} \subseteq \bigcup_{i \in I} A_i$, which, as $A_{\beta(0)}$ is denumerable, proves by [theorem: 6.27] that $\bigcup_{i \in I} A_i$ is not finite. So we must have that $\bigcup_{i \in I} A_i$ is enumerable. □

Theorem 6.62. *If $\{A_i\}_{i \in I}$ is such that I is denumerable and $\forall i \in I$ A_i is denumerable then $\bigcup_{i \in I} A_i$ is denumerable. In other words every union of a denumerable family of denumerable sets is denumerable.*

Proof. As I is denumerable there exist a bijection $\beta: \mathbb{N}_0 \rightarrow I$. Further as $\forall i \in I$ A_i is denumerable there exist a bijection $\alpha_i: \mathbb{N}_0 \rightarrow A_i$. Define now the function

$$g: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ by } g(n, m) = \alpha_{\beta(n)}(m)$$

Now if $y \in \bigcup_{i \in I} A_i$ there exist a $l \in I$ such that $y \in A_l$, as β is bijective there exists a $n \in \mathbb{N}_0$ such that $\beta(n) = l$. As $\alpha_l: \mathbb{N}_0 \rightarrow A_l$ is a bijection there exist a $m \in \mathbb{N}_0$ such that $\alpha_l(m) = y$. So

$$g(n, m) = \alpha_{\beta(n)}(m) = \alpha_l(m) = y$$

proving that

$$g: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ is surjective}$$

Now by [theorem: 6.56] there exist a bijection $\gamma: \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{N}_0$ so that

$$g \circ \gamma: \mathbb{N}_0 \to \bigcup_{i \in I} A_i \text{ is surjective}$$

Using [theorem: 6.10] we have that $\bigcup_{i \in I} A_i \preccurlyeq \mathbb{N}_0$ which by [definition: 6.3] gives that $\exists E \subseteq \mathbb{N}_0$ such that $\bigcup_{i \in I} A_i \approx \mathbb{N}_0$. Using [theorem: 6.55] we have that E is either finite or E is denumerable so that $\bigcup_{i \in I} A_i$ is either finite or denumerable. As $A_{\beta(0)} \subseteq \bigcup_{i \in I} A_i$ and $A_{\beta(0)}$ is denumerable it follows from [theorem: 6.27] that $\bigcup_{i \in I} A_i$ is not finite. So we must have that $\bigcup_{i \in I} A_i$ is enumerable. □

6.2.4 Countable Sets

Remember that a countable set is a set that is either finite or denumerable.

Theorem 6.63. *Every subset of a denumerable set is countable*

Proof. This follows from [theorem: 6.55] and the definition of countable sets. □

Theorem 6.64. *Every subset of a countable set is countable*

Proof. If A is countable then A is either denumerable or finite. If A is finite then by [theorem: 6.40] every subset of A is finite hence countable. If A is denumerable then by [theorem: 6.63] every subset of A is countable. □

Theorem 6.65. *Let A be a non empty set then the following are equivalent:*

1. *A is countable*
2. *There exists a surjection $\beta: \mathbb{N}_0 \to A$*
3. *There exists a injection $\alpha: A \to \mathbb{N}_0$*
4. *There exist a denumerable set B and a injection $\alpha: A \to B$*

Proof.

1 ⇒ 2. If A is countable then we have either:

A is finite. Then $\exists n \in \mathbb{N}_0$ and a bijection $\alpha: n = S_n \to A$. As $A \neq \varnothing$ there exist a $a \in A$, this allows us to define the function

$$\beta: \mathbb{N}_0 \to A \text{ where } \beta(i) = \begin{cases} \alpha(i) \text{ if } i < n \\ a \text{ if } n \leqslant i \end{cases}$$

If $y \in A$ then as α is surjective we have that $\exists i \in S_n = n$ such that $\alpha(i) = y$ so that $\beta(i) = \alpha(i) = y$ proving hat $\beta: \mathbb{N}_0 \to A$ is surjective.

A is denumerable. Then $\mathbb{N}_0 \approx A$ so there exist a bijection, hence surjection, $\beta: \mathbb{N}_0 \to A$.

2 ⇒ 3. Given that there exists a surjection $\beta: \mathbb{N}_0 \to A$ and $A \neq \varnothing$ we have by [theorem: 6.9] the exisence of a injection $\alpha: A \to \mathbb{N}_0$.

3 ⇒ 4. As B is denumerable we have $\mathbb{N}_0 \approx B$ so there exist a bijection $\beta: \mathbb{N}_0 \to B$. by (3) there exist a injection $\alpha: A \to \mathbb{N}_0$, hence we have the injection $\beta \circ \alpha: A \to B$.

4 ⇒ 1. As B is denumerable there exist a bijection $\beta: B \to \mathbb{N}_0$ so that we have a injection $\beta \circ \alpha: A \to \mathbb{N}_0$. Using [theorem: 2.62] it follows that $\beta \circ \alpha: A \to (\beta \circ \alpha)(A) \subseteq \mathbb{N}_0$ is a bijection hence

$$A \approx (\beta \circ \alpha)(A) \subseteq \mathbb{N}_0$$

Using [theorem: 6.54] we have that $(\beta \circ \alpha)(A)$ is either fnite or denumerable. If $(\beta \circ \alpha)(A)$ is finite then there exist a $n \in \mathbb{N}_0$ such that $n \approx (\beta \circ \alpha)(A)$, hence $n \approx A$ proving that A is finite, hence countable. If $(\beta \circ \alpha)(A)$ is denumerable then $\mathbb{N}_0 \approx (\beta \circ \alpha)(A)$ so that $\mathbb{N}_0 \approx A$ proving that A is denumerable hence countable. So in allases we reach the conclusion that A is countable. □

Theorem 6.66. *If $\{A_i\}_{i \in I}$ is such that I is denumerable and $\forall i \in I$ A_i is countable then $\bigcup_{i \in I} A_i$ is countable. In other words every union of a denumerable family of countable sets is countable.*

Proof. As I is denumerable there exist a bijection $\beta: \mathbb{N}_0 \rightarrow I$. Further as $\forall i \in I$ A_i is denumerable there exist a surjection $\alpha_i: \mathbb{N}_0 \rightarrow A_i$ [see theorem: 6.65]. Define now the function

$$g: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ by } g(n,m) = \alpha_{\beta(n)}(m)$$

Now if $y \in \bigcup_{i \in I} A_i$ there exist a $l \in I$ such that $y \in A_l$, as β is bijective there exists a $n \in \mathbb{N}_0$ such that $\beta(n) = l$. As $\alpha_l: \mathbb{N}_0 \rightarrow A_l$ is a surjection there exist a $m \in \mathbb{N}_0$ such that $\alpha_l(m) = y$. So

$$g(n,m) = \alpha_{\beta(n)}(m) = \alpha_l(m) = y$$

which proves that

$$g: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ is surjective}$$

Now by [theorem: 6.56] there exist a bijection $\gamma: \mathbb{N}_0 \rightarrow \mathbb{N}_0 \times \mathbb{N}_0$ so that

$$g \circ \gamma: \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ is surjective}$$

Using [theorem: 6.65] it follows that $\bigcup_{i \in I} A_i$ is countable. □

Theorem 6.67. *If $\{A_i\}_{i \in I}$ is such that $I \neq \varnothing \wedge I$ is finite and $\forall i \in I$ A_i is countable then $\bigcup_{i \in I} A_i$ is countable. In other words the union of a finite family of countable sets is countable. If in addition $\forall i \in I$ $A_i \neq \varnothing$ and $\forall i, j \in \mathbb{N}_0$ with $i \neq j$ $A_i \bigcap A_j = \varnothing$ then $\bigcup_{i \in I} A_i$ is denumerable.*

Proof. As I is finite and non empty there exist $n_0 \in \mathbb{N}_0 \setminus \{0\}$ and a bijection $\beta: n_0 \rightarrow I$. Further as $\forall i \in I$ A_i is countable there exist a surjection $\alpha_i: \mathbb{N}_0 \rightarrow A_i$ [see theorem: 6.65].] Define now the function

$$g: n_0 \times \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ by } g(n,m) = \alpha_{\beta(n)}(m)$$

Now if $y \in \bigcup_{i \in I} A_i$ there exist a $l \in I$ such that $y \in A_l$, as β is bijective there exists a $n \in n_0$ such that $\beta(n) = l$. As $\alpha_l: \mathbb{N}_0 \rightarrow A_l$ is a surjection there exist a $m \in \mathbb{N}_0$ such that $\alpha_l(m) = y$. So

$$g(n,m) = \alpha_{\beta(n)}(m) = \alpha_l(m) = y$$

which proves that

$$g: n_0 \times \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ is surjective}$$

Now by [theorem: 6.59] there exist a bijection $\gamma: \mathbb{N}_0 \rightarrow n_0 \times \mathbb{N}_0$ so that

$$g \circ \gamma: \mathbb{N}_0 \rightarrow \bigcup_{i \in I} A_i \text{ is surjective}$$

Using [theorem: 6.65] it follows that

$$\bigcup_{i \in I} A_i \text{ is countable}$$

Further if $\forall i \in I$ $A_i \neq \varnothing$ and $\forall i, j \in \mathbb{N}_0$ with $i \neq j$ $A_i \bigcap A_j = \varnothing$ then we can use a consequence of the axiom of choice [see theorem: 3.121] to find a function

$$\mathcal{C}: I \rightarrow \bigcup_{i \in I} A_i \text{ such that } \forall i \in I\ \mathcal{C}(i) \in A_i$$

If $\mathcal{C}(i) = \mathcal{C}(j)$ then $\mathcal{C}(i) \in A_i$ and $\mathcal{C}(i) = C(j) \in A_j$ so that $\mathcal{C}(i) \in A_i \bigcap A_j \Rightarrow A_i \bigcap A_j \neq \varnothing$. hence we must have $i = j$ [if $i \neq j$ then $A_i \bigcap A_j = \varnothing$]. So $\mathcal{C}: I \rightarrow \bigcup_{i \in I} A_i$ is a injection and $\mathcal{C}: I \rightarrow \mathcal{C}(I)$ is a bijection or $I \approx \mathcal{C}(I)$, as I is countable it follows from [theorem: 6.24] that $\mathcal{C}(I)$ is denumerable. As $\mathcal{C}(I) \subseteq \bigcup_{i \in I} A_i$ we have by [theorem: 6.27] that $\bigcup_{i \in I} A_i$ is not finite, so as $\bigcup_{i \in I} A_i$ is countable we have $\bigcup_{i \in I} A_i$ is denumerable. □

Theorem 6.68. *If A, B are countable sets then we have $A \times B$ is countable.*

Proof. For A, B we have the following possibilities:

***A* is finite and *B* is finite.** Then by [theorem: 6.38] $A \times B$ is finite hence countable.

***A* is finite and *B* is denumerable.** Then by [theorem: 6.60] $A \times B$ is denumerable hence countable.

***A* is denumerable and *B* is finite.** Then by [theorem: 6.60] $A \times B$ is denumerable hence countable.

***A* is denumerable and *B* is denumerable.** Then by [theorem: 6.58] $A \times B$ is denumerable hence countable. □

Lemma 6.69. *Let $n \in \mathbb{N}_0 \setminus \{0\}$ and $\{A_i\}_{i \in S_n}$ such that $\forall i \in S_n$ A_i is countable then $\prod_{i \in S_n} A_i$ is countable.*

Proof. We proof this by induction, so define

$$S = \left\{ n \in \{1, \ldots, \infty\} | \text{If } \{A_i\}_{i \in S_n} \text{ satisfies } \forall i \in S_n \ A_i \text{ is countable then } \prod_{i \in S_n} A_i \text{ is countable} \right\}$$

then we have:

$1 \in S$. As $S_1 = \{0\}$ we can use [example: 2.120] to find a bijection $\beta: A_0 \rightarrow \prod_{i \in \{0\}} A_i = \prod_{i \in S_1} A_i$ proving that $A_0 \approx \prod_{i \in S_1} A_i$, hence $\prod_{i \in S_1} A_i$ is countable [see theorem" 6.24].

$n \in S \Rightarrow n + 1 \in S$. Let $\{A_i\}_{i \in S_{n+1}}$ be such that $\forall i \in S_{n+1}$ A_i is countable. As $n \in S$ we have that $\prod_{i \in S_n} A_i$ is countable, so by [theorem: 6.68] we have that $(\prod_{i \in S_n} A_i) \times A_n$ is countable. Finally by [theorem: 6.51] we have $\prod_{i \in S_{n+1}} A_i \approx (\prod_{i \in S_n} A_i) \times A_n$ so that $\prod_{i \in S_{n+1}} A_i$ is countable [see theorem: 6.24]. Hence $n + 1 \in S$

Mathematical induction proves then that $S = \{1, \ldots, \infty\}$ proving the theorem. □

Theorem 6.70. *If I is non empty and finite and $\{A_i\}_{i \in I}$ such that $\forall i \in I$ A_i is countable then $\prod_{i \in I} A_i$ is countable.*

Proof. As I is finite and non empty there exists a $n \in \mathbb{N}_0 \setminus \{0\}$ such that $n \approx I$ hence there exist a bijection $f: n = S_n \rightarrow I$, Using [theorem: 2.125] there exists a bijection $\beta: \prod_{i \in I} A_i \rightarrow \prod_{i \in S_n} A_{f(i)}$ so that $\prod_{i \in S_n} A_{f(i)} \approx \prod_{i \in I} A_i$. Using the previous lemma [lemma: 6.69] $\prod_{i \in S_n} A_{f(i)}$ is countable, hence by [theorem: 6.24] $\prod_{i \in I} A_i$ is countable. □

Chapter 7
The integer numbers

TODO

7.1 Definition and arithmetic

One major defect of $\mathbb{N}_0$ is that $n-m$, defined to be the unique number such that $(n-m)+m=n$, is only defined for $m \leqslant n$. If this limitation didn't exist then we can easely find a inverse for a number n, just take $-n=0-n$, then $(-n)+n=(0-n)+n=0$. So how to extend $\mathbb{N}_0$ so that $n-m$ always exist, first note that $n-m$ consist of two number so we can always write this as a pair. Then (n,m) is to be interpreted as $n-m$, members of $\mathbb{N}_0$ are then represented by $(n,0)$ as $n-0=n$. However we hit a problem, the same number has many representations as a pair, for example, as $3=3-0=4-1=5-2$, etc, the natural number 3 would have the representations $(3,0)$, $(4,1), (5,2)$, etc. How can we solve this? If (n,m) and (n',m') are two representations of the same number then in our formal interpretion we would have that $n-m=n'-m'$ which formally gives $n+m'=m+n'$. So it is natural to say that two pairs (n,m), (n',m') satisfying $n+m'=m+n'$ represent the same number. The way to do this, is to define a equivalence relation whose equivalence classes are the integers. This is what we will do in this chapter.

Theorem 7.1. *The relation* $\sim \subseteq (\mathbb{N}_0 \times \mathbb{N}_0) \times (\mathbb{N}_0 \times \mathbb{N}_0)$ *defined by*

$$\sim = \{((n,m),(n',m')) | n+m'=m+n'\}$$

is a equivalence relation.

Proof.

reflexivity. If $(n,m) \in \mathbb{N}_0 \times \mathbb{N}_0$ then $n+m \underset{\text{[theorem: 5.33]}}{=} m+n$ so that $(n,m) \approx (n,m)$.

symmetry. If $(n,m) \sim (n',m')$ then $n+m'=m+n' \underset{\text{[theorem: 5.33]}}{\Rightarrow} n'+m=m'+n$ so that $(n',m') \sim (n,m)$.

transitivity. We have

$$\begin{aligned} (n,m) \sim (n',m') \wedge (n',m') \sim (n'',m'') &\Rightarrow n+m'=m+n' \wedge n'+m''=m'+n'' \\ &\Rightarrow (n+m')+(n'+m'')=(m+n')+(m'+n'') \\ &\Rightarrow (n+m'')+(m'+n')=(m+n'')+(n'+m') \\ &\Rightarrow (n+m'')+(n'+m')=(m+n'')+(n'+m') \\ &\Rightarrow (n+m'')=(m+n'') \end{aligned}$$

so that $(n,m) \sim (n'',m'')$. $\square$

Next we define the set of integers.

Definition 7.2. *The set of integers* $\mathbb{Z}$ *is defined by* $\mathbb{Z}/\sim$ *or in other words*

$$\mathbb{Z} = \{\sim[(n,m)] | (n,m) \in \mathbb{N}_0 \times \mathbb{N}_0\}$$

Theorem 7.3. *If* $\sim[(n,m)] \in \mathbb{Z}$ *then if* $k \in \mathbb{N}_0$ *we have* $\sim[(n,m)] = \sim[(n+k,m+k)]$

Proof. $n+(m+k)=(n+m)+k=(m+n)+k=m+(n+k)$ so that $(n,m) \sim (n+k,m+k)$. Hence by [theorem: 3.11] $\sim[(n,m)] = \sim[(n+k,m+k)]$. $\square$

Theorem 7.4. *If* $\sim[(n,m)], \sim[(r,s)], \sim[(n',m')]$ *and* $\sim[(r',s')]$ *are elements of* $\mathbb{Z}$ *such that* $\sim[(n,m)] = \sim[(n',m')]$ *and* $\sim[(r,s)] = \sim[(r',s')]$ *then* $\sim[(n+r,m+s)] = \sim[(n'+r',m'+s')]$

Proof. As $\sim[(n,m)] = \sim[(n',m')] \wedge \sim[(r,s)] = \sim[(r',s')]$ we have

$$n+m'=m+n' \wedge r+s'=s+r' \tag{7.1}$$

then

$$\begin{array}{rcl}(n+r)+(m'+s') & = & (n+m')+(r+s') \\ & \underset{[\text{eq: } 7.1]}{=} & (m+n')+(s+r') \\ & = & (m+s)+(n'+r')\end{array}$$

so that $(n+r,m+s) \sim (n'+r',m'+s')$ proving that

$$\sim[(n+r,m+s)] = \sim[(n'+r',m'+s')]$$

□

The above ensure that the following definition is well defined:

Definition 7.5. *The sum operator* $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *is defined by*

$$\sim[(n,m)] + \sim[(r,s)] = \sim[(n+r,m+s)]$$

Lemma 7.6. *If* $n \in \mathbb{N}_0$ *then* $\sim[(n,n)] = \sim[(0,0)]$

Proof. As $n+0=n+0$ we have $(n,n) \sim (0,0)$ so that $\sim[(n,n)] = \sim[(0,0)]$. □

Remark 7.7. Be carefull in the above definition, because the same symbol $+$ is used for the sum in $\mathbb{N}_0$ and the sum in $\mathbb{Z}$. We use context to indicate which operator is used. If $n,m \in \mathbb{N}_0$ then $n+m$ is the sum defined for the natural numbers and if $n,m \in \mathbb{Z}$ then $n+m$ is the sum defined in $\mathbb{Z}$. So context is important. Another reuse of the same symbol is for the neutral element 0, so if $n \in \mathbb{N}_0$ then 0 in $n+0$ is the neutral element of $\mathbb{N}_0$ and if $n \in \mathbb{Z}$ then 0 in $n+0$ is the neutral element of $\mathbb{Z}$.

Set	Expression	Operator
$n,m \in \mathbb{N}_0$	n+m	sum in $\langle \mathbb{N}_0, + \rangle$
$n,m \in \mathbb{N}_0$	$n \cdot m$	product in $\langle \mathbb{N}_0, \cdot \rangle$

Theorem 7.8. ($\langle \mathbb{Z}, + \rangle$ is a Abelain group) *so*

Associativity. $\forall n,m,k \in \mathbb{Z}$ *we have* $(n+m)+k = n+(m+k)$.

Neutral element. $\forall n \in \mathbb{Z}$ *we have that* $n+0=0+n$ *where* $0 = \sim[(0,0)]$.

Inverse element. $\forall n \in \mathbb{Z}$ *there exist a inverse element* $-n$ *such that* $(-n)+n=0=n+(-n)$. *More specifically if* $x = \sim[(n,m)]$ *then* $-x = [(m,n)]$.

Commutativity. $\forall n,m \in \mathbb{N}_0$ *we have* $n+m=m+n$.

Proof.

Associativity. If $n = \sim[(n_1,m_1)]$,$m = \sim[(n_2,m_2)]$ and $k = \sim[(n_3,m_3)]$ then we have

$$\begin{array}{rcl}(n+m)+k & = & (\sim[(n_1,m_1)] + \sim[(n_2,m_2)]) + \sim[(n_3,m_3)] \\ & = & \sim[(n_1+n_2, m_1+m_2)] + \sim[(n_3,m_3)] \\ & = & [\sim((n_1+n_2)+n_3, (m_1+m_2)+m_3)] \\ & = & \sim[(n_1+(n_2+n_3), m_1+(m_2+m_3))] \\ & = & \sim[(n_1,m_1)] + \sim[(n_2+n_3, m_2+m_3)] \\ & = & \sim[(n_1,m_1)] + (\sim[(n_2,m_2)] + \sim[(n_3,m_3)]) \\ & = & n+(m+k)\end{array}$$

Commutatitivity. If $n = \sim[(n_1,m_1)]$ and $m = \sim[(n_2,m_2)]$ then

$$\begin{array}{rcl}\sim[(n_1,m_1)] + \sim[(n_2,m_2)] & = & \sim[(n_1+n_2, m_1+m_2)] \\ & = & \sim[(n_2+n_1, m_2+m_1)] \\ & = & \sim[(n_2,m_2)] + \sim[(n_1,m_1)]\end{array}$$

Neutral element. If $k = \sim[(n,m)] \in \mathbb{Z}$ then

$$\begin{aligned} k+0 &\underset{\text{commutativity}}{=} 0+n \\ &= \sim[(n,m)] + \sim[(0,0)] \\ &= \sim[(n+0, m+0)] \\ &= \sim[(n,m)] \\ &= k \end{aligned}$$

Inverse element. If $k = \sim[(n,m)]$

$$\begin{aligned} k+(-k) &\underset{\text{commutativity}}{=} (-k)+k \\ &= \sim[(m,n)] + \sim[(n,m)] \\ &= \sim[(m+n, n+m)] \\ &= \sim[(n+m, n+m)] \\ &\underset{\text{[throrem: 7.6]}}{=} \sim[(0,0)] \end{aligned}$$

□

Remark 7.9. Next we are gooing to define multiplication in $\mathbb{Z}$, again we will reuse symbols for simplicity, So if $n, m \in \mathbb{N}_0$ then $n \cdot m$ is mulitiplication in $\mathbb{N}_0$ and if $n, m \in \mathbb{N}_0$ then $n \cdot m$ is multiplication in $\mathbb{Z}$. Likewise 1 could be the neutral element in $\mathbb{N}_0$ or $\mathbb{Z}$.

Definition 7.10. *Let $n, m \in \mathbb{Z}_0^+$ then we have $n - m = n + (-m)$.*

Theorem 7.11. *If $\sim[(n,m)], \sim[(r,s)], \sim[(n',m')]$ and $\sim[(r',s')]$ are elements of $\mathbb{Z}$ such that $\sim[(n,m)] = \sim[(n',m')]$ and $\sim[(r,s)] = \sim[(r',s')]$ then*

$$\sim[(n \cdot r + m \cdot s, m \cdot r + n \cdot s)] = \sim[(n' \cdot r' + m' \cdot s', m' \cdot r' + n' \cdot s')]$$

Proof. As $\sim[(n,m)] = \sim[(n',m')] \wedge \sim[(r,s)] = \sim[(r',s')]$ we have

$$n + m' = m + n' \wedge r + s' = s + r' \tag{7.2}$$

So we have

$$\begin{aligned} n \cdot r + m' \cdot r &= (n+m') \cdot r \\ &\underset{\text{[eq: 7.2]}}{=} (m+n') \cdot r \\ &= m \cdot r + n' \cdot r \\ m \cdot s + n' \cdot s &= (m+n') \cdot s \\ &\underset{\text{[eq: 7.2]}}{=} (n+m') \cdot s \\ &= n \cdot s + m' \cdot s \\ m' \cdot s + m' \cdot r' &= m' \cdot (s+r') \\ &\underset{\text{[eq: 7.2]}}{=} m' \cdot (r+s') \\ &= m' \cdot r + m' \cdot s' \\ n' \cdot r + n' \cdot s' &= n' \cdot (r+s') \\ &\underset{\text{[eq: 7.2]}}{=} n' \cdot (s+r') \\ &= n' \cdot s + n' \cdot r' \end{aligned}$$

so after summing, here common terms are underlined,

$$\begin{aligned} &n \cdot r + \underbrace{m' \cdot r}_{1} + m \cdot s + \underbrace{n' \cdot s}_{2} + \underbrace{m' \cdot s}_{3} + m' \cdot r' + \underbrace{n' \cdot r}_{4} + n' \cdot s' \;= \\ &m \cdot r + \underbrace{n' \cdot r}_{4} + n \cdot s + \underbrace{m' \cdot s}_{3} + \underbrace{m' \cdot r}_{1} + m' \cdot s' + \underbrace{n' \cdot s}_{2} + n' \cdot r' \end{aligned}$$

Using [theorem: 5.43] to eliminate common terms in the above gives:

$$n \cdot r + m \cdot s + m' \cdot r' + n' \cdot s' \;=\; m \cdot r + n \cdot s + m' \cdot s' + n' \cdot r'$$

So that

$$(n\cdot r+m\cdot s, m\cdot r+n\cdot s) \sim (n'\cdot r'+m'\cdot s', m'\cdot r'+n'\cdot s')$$

Hence

$$\sim[(n\cdot r+m\cdot s, m\cdot r+n\cdot s)]=\sim[(n'\cdot r'+m'\cdot s', m'\cdot r'+n'\cdot s')]$$ □

The above theorem ensures that the following definition is sensible.

Definition 7.12. *The muliplication operator* $\cdot:\mathbb{Z}\times\mathbb{Z}\rightarrow\mathbb{Z}$ *is defined by*

$$\sim[(n,m)]\cdot\sim[(r,s)]=\sim[(n\cdot r+m\cdot s, m\cdot r+n\cdot s)]$$

Theorem 7.13. $\langle\mathbb{Z},+,\cdot\rangle$ *is a* ***integral domain*** *[definition: 4.28] more in detail:*

1. $\langle\mathbb{Z},+\rangle$ *is a abelian group [see: 7.8]*
2. $\langle\mathbb{Z},\cdot\rangle$ *is a* ***Abelian semi-group****.*

   Associativity. $\forall n,m,k\in\mathbb{Z}$ *we have* $n\cdot(m\cdot k)=(n\cdot m)\cdot k$

   Neutral Element. *There exist a* $1=\sim[(1,0)]$ *such that* $\forall n\in\mathbb{N}_0$ *we have* $n\cdot 1=n=1\cdot n$.

   Commutativity. $\forall n,m\in\mathbb{Z}$ *we have* $n\cdot m=m\cdot n$.
3. *Further we have:*

   Distributivity. $\forall n,m,k\in\mathbb{Z}$ *we have* $n\cdot(m+k)=n\cdot m+n\cdot k$

   There does not exist a zero divisor. *If* $n,m\in\mathbb{Z}$ *is such that* $n\cdot m=0\Rightarrow n=0\vee m=0$
4. *Additional we have also that* $(-1)\cdot(-1)$

Proof.

1. This is already proved in [theorem: 7.8].
2.

   Commutatitivity. If $\sim[(n,m)],\sim[(r,s)]\in\mathbb{Z}$ we have

$$\begin{aligned}\sim[(n,m)]\cdot\sim[(r,s)] &= \sim[(n\cdot r+m\cdot s, m\cdot r+n\cdot s)]\\ &= \sim[(r\cdot n+s\cdot m, s\cdot n+r\cdot m)]\\ &= \sim[(r,s)]\cdot\sim[(n,m)]\end{aligned}$$

   Associativity. Let $\sim[(a,b)],\sim[(c,d)],\sim[(e,f)]\in\mathbb{Z}$ then

$$\begin{aligned}&\sim[(a,b)]\cdot(\sim[(c,d)]\cdot\sim[(e,f)]) =\\ &\sim[(a,b)]\cdot(\sim[(c\cdot e+d\cdot f, d\cdot e+c\cdot f)]) =\\ &\sim[(a\cdot(c\cdot e+d\cdot f)+b\cdot(d\cdot e+c\cdot f), b\cdot(c\cdot e+d\cdot f)+a\cdot(d\cdot e+c\cdot f))] =\\ &\sim\left[\left(\underbrace{a\cdot(c\cdot e)}_{1}+\underbrace{a\cdot(d\cdot f)}_{2}+\underbrace{b\cdot(d\cdot e)}_{3}+\underbrace{b\cdot(c\cdot f)}_{4}, \underbrace{b\cdot(c\cdot e)}_{5}+\underbrace{b\cdot(d\cdot f)}_{6}+\underbrace{a\cdot(d\cdot e)}_{7}+\right.\right.\\ &\left.\left.\underbrace{a\cdot(c\cdot f)}_{8}\right)\right] =\\ &\sim\left[\left(\underbrace{(a\cdot c)\cdot e}_{1}+\underbrace{(b\cdot d)\cdot e}_{3}+\underbrace{(b\cdot c)\cdot f}_{4}+\underbrace{(a\cdot d)\cdot f}_{2}, \underbrace{(b\cdot c)\cdot e}_{5}+\underbrace{(a\cdot d)\cdot e}_{7}+\underbrace{(a\cdot c)\cdot f}_{8}+\right.\right.\\ &\left.\left.\underbrace{(b\cdot d)\cdot f}_{6}\right)\right]\\ &\sim[((a\cdot c+b\cdot d)\cdot e+(b\cdot c+a\cdot d)\cdot f), (b\cdot c+a\cdot d)\cdot e+(a\cdot c+b\cdot d)\cdot f] =\\ &\sim[(a\cdot c+b\cdot d, b\cdot c+a\cdot d)]\cdot\backsim[(e,f)] =\\ &(\sim[(a,b)]\cdot\sim[(c,d)])\cdot\sim[(e,f)]\end{aligned}$$

Neutral element. If $n = \sim[(n,m)] \in \mathbb{Z}$ then we have

$$\begin{array}{rcl} n \cdot 1 & \underset{\text{commutativity}}{=} & 1 \cdot n \\ & = & \sim[(1,0)] \cdot \sim[(n,m)] \\ & = & \sim[(1 \cdot n + 0 \cdot m, 0 \cdot n + 1 \cdot m)] \\ & = & \sim(n,m) \end{array}$$

3. Further we have:

Distributivity. If $\sim[(a,b)], \sim[(c,d)], \sim[(e,f)] \in \mathbb{Z}$ then

$$\begin{array}{rl} \sim[(a,b)] \cdot (\sim[(c,d)] + \sim[(e,f)]) & = \\ \sim[(a,b)] \cdot \sim[(c+e, d+f)] & = \\ \sim[(a \cdot (c+e) + b \cdot (d+f), b \cdot (c+e) + a \cdot (d+f))] & = \\ \sim\left[\left(\underbrace{a \cdot c}_{1} + \underbrace{a \cdot e}_{2} + \underbrace{b \cdot d}_{3} + \underbrace{b \cdot f}_{4}, \underbrace{b \cdot c}_{5} + \underbrace{b \cdot e}_{6} + \underbrace{a \cdot d}_{7} + \underbrace{a \cdot f}_{8}\right)\right] & = \\ \sim\left[\left(\underbrace{a \cdot c}_{1} + \underbrace{b \cdot d}_{3} + \underbrace{a \cdot e}_{2} + \underbrace{b \cdot f}_{4}, \underbrace{b \cdot c}_{5} + \underbrace{a \cdot d}_{7} + \underbrace{b \cdot e}_{6} + \underbrace{a \cdot f}_{8}\right)\right] & = \\ \sim[(a \cdot c + b \cdot d, b \cdot c + a \cdot d)] + \sim[(a \cdot e + b \cdot f, b \cdot e + a \cdot f)] & = \\ \sim[(a,b)] \cdot \sim[(c,d)] + \sim[(a,b)] \cdot \sim[(e,f)] & = \end{array}$$

There does not exist a zero divisor. Let $n = \sim\{(a,b)\}$, $m = \sim[(c,d)]$ such that $n \cdot m = 0$ then

$$\sim[(a,b)] \cdot \sim[(c,d)] = \sim[(a \cdot c + b \cdot d, b \cdot c + a \cdot d)] = \sim[(0,0)]$$

so we have that $(a \cdot c + b \cdot d) + 0 = (b \cdot c + a \cdot d) + 0$ giving

$$a \cdot c + b \cdot d = b \cdot c + a \cdot d \tag{7.3}$$

Assume that $n \neq 0$ then $\sim[(a,b)] \neq \sim[(0,0)]$ so that $a + 0 \neq b + 0$ so that $a \neq b$, hence we have te following cases to consider:

***a* < *b*.** Then using [theorem: 5.60] there exists a $k \in \mathbb{N}_0 \setminus \{0\}$ such that $a + k = b$, so substituting this in [eq: 7.3] gives

$$\begin{array}{rcl} a \cdot c + (a+k) \cdot d = (a+k) \cdot c + a \cdot d & & \Rightarrow \\ \underbrace{a \cdot c}_{1} + \underbrace{a \cdot d}_{2} + k \cdot d = \underbrace{a \cdot c}_{1} + k \cdot c + \underbrace{a \cdot d}_{2} & & \Rightarrow \\ k \cdot d = k \cdot c & & \underset{k \neq 0 \wedge [\text{theorem: } 5.76]}{\Rightarrow} \\ d = c & & \end{array}$$

So $m = \sim[(c,d)] = \sim[(d,d)] \underset{[\text{theorem: } 7.6]}{=} ![(0,0)] = 0.$

***b* < *a*.** Then using [theorem: 5.60] there exists a $k \in \mathbb{N}_0 \setminus \{0\}$ such that $b + k = a$, so substituting this in [eq: 7.3] gives

$$\begin{array}{rcl} (b+k) \cdot c + b \cdot d = b \cdot c + (b+k) \cdot d & & \Rightarrow \\ \underbrace{b \cdot c}_{1} + k \cdot c + \underbrace{b \cdot d}_{2} = \underbrace{b \cdot c}_{1} + \underbrace{b \cdot d}_{2} + k \cdot d & & \Rightarrow \\ k \cdot c = k \cdot d & & \underset{k \neq 0 \wedge [\text{theorem: } 5.76]}{\Rightarrow} \\ c = d & & \end{array}$$

So $m = \sim[(c,d)] = \sim[(d,d)] \underset{[\text{theorem: } 7.6]}{=} [(0,0)] = 0.$

So if $n \cdot m = 0$ then we have either $n \neq 0$ but then $m = 0$ or $n = 0$ proving that $n \cdot m = 0 \Rightarrow n = 0 \vee m = 0$.

4. As $1 = \sim[(1,0)]$ we heve by [theorem: 7.8] that $-1 = \sim[(0,1)]$ so that

$$(-1)\cdot(-1) = \sim[(0,1)]\cdot\sim[(0,1)] = \sim[(0\cdot 0+1\cdot 1, 1\cdot 0+0\cdot 1)] = \sim[(1,0)] = 1 \qquad \square$$

Lemma 7.14. *$\forall n \in \mathbb{N}_0 \setminus \{0\}$ we have that $\sim[(n,0)] \neq 0$*

Proof. We prove this by contradiction so assume that $\sim[(n,0)] = 0 = \sim[(0,0)]$ then $n+0=0 \Rightarrow n=0$ contradicting $n \in \mathbb{N}_0 \setminus \{0\}$. So $\sim[(n,0)] \neq 0$. $\square$

Corollary 7.15. *$\forall z \in \mathbb{Z}$ such that $z = -z$ we have $z = 0$*

Proof. If $z = -z$ we have that $z + z = (-z) + z = 0$. So $(1+1)\cdot z = z\cdot 1 + z\cdot 1 = z + z = 0$, hence

$$(1+1)\cdot z = 0$$

As $1+1 = \sim[(1,0)] + \sim[(1,0)] = \sim[(2,0)]$ and $2 = 0$ we have by [corollary: 7.14] that $1+1 \neq 0$, using [theorem: 7.13] on the above proves then that $Z = 0$. $\square$

Theorem 7.16. (Absorbing element) *If $z \in \mathbb{Z}$ then $0\cdot n = 0 = n\cdot 0$*

Proof. Let $z = \sim[(n,m)]$ then

$$\begin{aligned} n\cdot 0 &\underset{\text{commutativity}}{=} 0\cdot n \\ &= \sim[(0,0)]\cdot\sim[(n,m)] \\ &= \sim[(0\cdot n+0\cdot m, 0\cdot n+0\cdot m)] \\ &= \sim[(0,0)] \\ &= 0 \end{aligned}$$

$\square$

Theorem 7.17. *If $z \in \mathbb{Z}$ then $(-1)\cdot z = -1$*

Proof. If $z = \sim[(n,m)]$ then we have by [theorem: 7.8] that $-z = \sim[(m,n)]$, further as $1 = \sim[(1,0)]$ we have $-1 = \sim[(0,1)]$. Hence

$$\begin{aligned} (-1)\cdot z &= \sim[(0,1)]\cdot\sim[(n,m)] \\ &= \sim[(0\cdot n+1\cdot m, 1\cdot n+0\cdot m)] \\ &= \sim[(m,n)] \\ &= -z \end{aligned}$$

$\square$

Theorem 7.18. *If $n, m \in \mathbb{Z}$ then $-(n\cdot m) = (-n)\cdot m = n\cdot(-m)$*

Proof.

$$\begin{aligned} -(n\cdot m) &\underset{\text{[theorem: 7.17]}}{=} (-1)\cdot(n\cdot m) \\ &\underset{\text{associativity}}{=} ((-1)\cdot n)\cdot m \\ &\underset{\text{[theorem: 7.17]}}{=} (-n)\cdot m \\ -(n,m) &\underset{\text{[theorem: 7.17]}}{=} (-1)\cdot(n\cdot m) \\ &\underset{\text{commutativity}}{=} (n\cdot m)\cdot(-1) \\ &\underset{\text{associativity}}{=} n\cdot(m\cdot(-1)) \\ &\underset{\text{commutativ}}{=} n\cdot((-1)\cdot m) \\ &\underset{\text{[theorem: 7.17]}}{=} n\cdot(-m) \end{aligned}$$

$\square$

Theorem 7.19. *Let $n, k, r \in \mathbb{Z}$ with $r \neq 0$ then $n \cdot r = k \cdot r$ implies $n = k$.*

Proof.

$$\begin{array}{lcl} n \cdot r = k \cdot r & \Rightarrow & n \cdot r + (-(k \cdot r)) = (k \cdot r) + (-(k \cdot r)) \\ & \Rightarrow & n \cdot r + (-(k \cdot r)) = 0 \\ & \underset{[\text{theorem: } 7.18]}{\Rightarrow} & n \cdot r + (-k) \cdot r = 0 \\ & \Rightarrow & (n + (-k)) \cdot r = 0 \end{array}$$

As by [theorem: 7.13] $\langle \mathbb{Z}, +, \cdot \rangle$ is a integral domain and $r \neq 0$ we have $n + (-k) = 0$ so that $(n + (-k)) + k = 0 + k$ or $n + ((-k) + k) = k$ proving $n = k$. □

We can use recursion [see: theorem 5.83] to define power in the set of integer

Definition 7.20. *Let $z \in \mathbb{Z}$ then $z^{(\cdot)}: \mathbb{N}_0 \rightarrow \mathbb{Z}$ $n \rightarrow z^n$ is defined by*

$$\begin{array}{rcl} z^0 & = & 1 \\ z^{n+1} & = & z \cdot z^n \end{array}$$

Theorem 7.21. *If $n, m \in \mathbb{N}_0$ and $z \in \mathbb{N}_0$ then $z^{n+m} = z^n \cdot z^m$*

Proof. This is proved by induction, so let $z \in \mathbb{Z}, n \in \mathbb{N}_0$ and define

$$S_{n,z} = \{m \in \mathbb{N}_0 | z^{n+m} = z^n \cdot z^m\}$$

then we have:

$\boldsymbol{0 \in S_{n,z}}$**.** Then $z^{n+0} = z^n = z^n \cdot 1 = z^n \cdot z^0$ proving that $0 \in S_{n,z}$.

$\boldsymbol{m \in S_{n,z} \Rightarrow m + 1 \in S_{n,z}}$**.** Then

$$\begin{array}{rcl} z^{n+(m+1)} & = & z^{(n+m)+1} \\ & = & z \cdot z^{(n+m)} \\ & = & z^{n+m} \cdot z \\ & \underset{m \in S_{n,z}}{=} & (z^n \cdot z^m) \cdot z \\ & = & z^n \cdot (z^m \cdot z) \\ & = & z^n \cdot (z \cdot z^m) \\ & = & z^n \cdot z^{m+1} \end{array}$$

proving that $m + 1 \in S_{n,z}$

Mathematical induction completes then the proof. □

Theorem 7.22. *Let $n \in \mathbb{N}_0$ then we have*

1. *If $n \neq 0$ then $0^n = 0$*
2. *$1^n = 1$*
3. *$(-1)^n = 1 \vee (-1)^n = -1$*
4. *$(-1)^{2 \cdot n} = 1$*
5. *$(-1)^{2 \cdot n + 1} = -1$*

Proof.

1. If $n \neq 0$ then $\exists m \in \mathbb{N}_0$ such that $n = m + 1$ so that $0^n = 0^{m+1} = 0 \cdot 0^m \underset{[\text{theorem: } 7.16]}{=} 0$
2. We proceed by induction, so let

$$S = \{n \in \mathbb{N}_0 | 1^n = 1\}$$

then we have:

$0\in S$. $1^0=1$ by definition proving that $0\in S$

$n\in S\Rightarrow n+1\in S$. $1^{n+1}=1\cdot 1^n \underset{n\in S}{=} 1\cdot 1$ proving that $n+1\in S$

3. Again we use induction, so let

$$S=\{n\in\mathbb{N}_0|(-1)^n=1\vee(-1)^n=-1\}$$

then we have:

$0\in S$. $(-1)^0=1$ proving that $0\in S$.

$n\in S\Rightarrow n+1\in S$. As $n\in S$ we have either:

$(-1)^n=1$. Then $(-1)^{n+1}=(-1)\cdot(-1)^n=(-1)\cdot 1=-1$ so the $n+1\in S$

$(-1)^n=-1$. Then $(-1)^{n+1}=(-1)\cdot(-1)^n=(-1)\cdot(-1) \underset{\text{[theroem: 7.13]}}{=} 1$ so that

4. $(-1)^{2\cdot n}=(-1)^{(1+1)\cdot n}=(-1)^{n+n} \underset{\text{[theorem: 7.21]}}{=} (-1)^n\cdot(-1)^n \underset{\text{[theorem: 7.13] and (3)}}{=} 1$

5. $(-1)^{2\cdot n+1}=(-1)\cdot(-1)^{2\cdot n} \underset{(4)}{=} (-1)\cdot 1=-1$

□

7.2 Order relation on the set of integers

First we define the set of non negative integers.

Definition 7.23. $\mathbb{Z}_0^+=\{\sim[(n,0)]|n\in\mathbb{N}_0\}\subseteq\mathbb{Z}$

We have the following properties for the set on non negative integers.

Theorem 7.24. *We have the following:*

1. *$\langle\mathbb{Z}_0^+,+\rangle$ is a sub semi-group of $\langle\mathbb{Z},+\rangle$ [hence by [theorem: 4.13] $\langle\mathbb{Z}_0^+,+\rangle$ is a Abelian semi-group].*
2. *$\langle\mathbb{Z}_0^+,\cdot\rangle$ is a sub semi-group of $\langle\mathbb{Z},\cdot\rangle$ $\langle\mathbb{Z},\cdot\rangle$ [hence by [theorem: 4.13] $\langle\mathbb{Z}_0^+,\cdot\rangle$ is a Abelian semi-group].*
3. *$i_{\mathbb{N}_0}:\mathbb{N}_0\rightarrow\mathbb{Z}_0^+$ defined by $i_{\mathbb{N}_0}(n)=\sim[(n,0)]$ forms a*
   a. *group isomorphism between $\langle\mathbb{N}_0,+\rangle$ and $\langle\mathbb{Z}_0^+,+\rangle$*
   b. *group isomorphism between $\langle\mathbb{N}_0,+\rangle$ and $\langle\mathbb{Z}_0^+,+\rangle$*
4. *For every $z\in\mathbb{Z}$ $\exists x,y\in\mathbb{Z}_0^+$ such that $z=x-y$*

Proof.

1. Let $z,z'\in\mathbb{Z}$ then $z=\sim[(n,0)]$ and $z'=\sim[(n',0)]$ so that

$$z+z'=\sim[(n,0)]+\sim[(n',0)]=\sim[(n+n',0+0)]=\sim[(n+n',0)]\in\mathbb{Z}_0^+$$

further

$$0=\sim[(0,0)]\in\mathbb{Z}_0^+.$$

Using [definition: 4.11] it follows that $\langle\mathbb{Z}_0^+,+\rangle$ is a sub semi-group of $\langle\mathbb{Z},+\rangle$.

2. Let $z,z'\in\mathbb{Z}$ then $z=\sim[(n,0)]$ and $z'=\sim[(n',0)]$ so that

$$z\cdot z'=\sim[(n,0)]\cdot\sim[(n',0)]=\sim[(n\cdot n'+0\cdot 0,0\cdot n'+n\cdot 0)]=\sim[(n\cdot n',0)]\in\mathbb{Z}_0^+$$

further

$$1=\sim[(1,9)]\in\mathbb{Z}_0^+$$

Using [definition: 4.11] it follows that $\langle\mathbb{Z}_0^+,+\rangle$ is a sub semi-group of $\langle\mathbb{Z},+\rangle$.

3. First we show that $i_{\mathbb{N}_0}$ is a bijection:

   injectivity. If $i_{\mathbb{N}_0}(n) = i_{\mathbb{N}_0}(m)$ then $\sim[(n,0)] = \sim[(m,0)]$ so that $n+0=0+m \Rightarrow n=m$.

   surjectivity. If $z \in \mathbb{Z}_0^+$ there exist a $n \in \mathbb{N}_0$ such that $z = \sim[(n,0)] = i_{\mathbb{N}_0}(n)$.

   Next we have:

   a. First $i_{\mathbb{N}_0}(n+m) = \sim[(n+m,0)] = \sim[(n,0)] + \sim[(m,0)] = i_{\mathbb{N}_0}(n) + i_{\mathbb{N}_0}(m)$. Second $i_{\mathbb{N}_0}(0) = \sim[(0,0)] = 1 \in \mathbb{Z}_0^+$.

   b. First

   $$\begin{aligned} i_{\mathbb{N}_0}(n) \cdot i_{\mathbb{N}_0}(m) &= \sim[(n,0)] \cdot \sim[(m,0)] \\ &= \sim[(n \cdot m + 0 \cdot m, 0 \cdot n + n \cdot 0)] \\ &= \sim[(n \cdot m, 0)] \\ &= i_{\mathbb{N}_0}(n \cdot m) \end{aligned}$$

   Second $i_{\mathbb{N}_0}(1) = \sim[(1,0)] = 1 \in \mathbb{Z}_0^+$.

4. Let $z \in \mathbb{Z}$ then $z = \sim[(n,m)]$ take $x = \sim[(n,0)] \in \mathbb{Z}_0^+$ and $y = \sim[(m,0)] \in \mathbb{Z}_0^+$ then we have

   $$x - y = x + (-y) = \sim[(n,0)] + \sim[(0,m)] = \sim[(n,m)] = z$$ □

Next we define the set of non positive number.

Definition 7.25. $\mathbb{Z}_0^- = \{-n | n \in \mathbb{Z}_0^+\} = \{(0,n) | n \in \mathbb{N}_0\} \subseteq \mathbb{Z}$

Definition 7.26. $\mathbb{Z}^+ = \mathbb{Z}_0^+ \setminus \{0\}$ *and* $\mathbb{Z}^- = \mathbb{Z}_0^- \setminus \{0\}$

The following theorem shows the relation between $\mathbb{Z}_0^+$ and $\mathbb{Z}_0^-$.

Theorem 7.27. $\mathbb{Z} = \mathbb{Z}_0^+ \bigcup \mathbb{Z}_0^-$ *and* $\{0\} = \mathbb{Z}_0^+ \bigcap \mathbb{Z}_0^-$

Proof. As $\mathbb{Z}_0^+ \subseteq \mathbb{Z}$ and $\mathbb{Z}_0^- \subseteq \mathbb{Z}$ then

$$\mathbb{Z}_0^+ \bigcup \mathbb{Z}_9^- \subseteq \mathbb{Z} \tag{7.4}$$

Let $z \in \mathbb{Z}$ then $\exists n, m \in \mathbb{N}_0$ such that $z = \sim[(n,m)]$ then for n, m we have either:

***n* ⩽ *m*.** then using [theorem: 5.62] there exist a $k \in \mathbb{N}_0$ such that $m = n + k$ so that

$$z = \sim[(n, n+k)] \tag{7.5}$$

Now for $(0,k)$ and $(n, n+k)$ we have $0 + (n+k) = n + k$ so that $(0,k) \sim (n, n+k)$ proving that $\sim[(0,k)] = \sim[(n,n+k)] \underset{\text{[eq: 7.5}}{=} z$, proving that $z \in \mathbb{Z}_0^- \subseteq \mathbb{Z}_0^+ \bigcup \mathbb{Z}_0^-$.

***m* < *n*.** Then using [theorem: 5.62] there exist a $k \in \mathbb{N}_0$ such that $n = m + k$ so that

$$z = \sim[(m+k, m)] \tag{7.6}$$

Now for $(k,0)$ and $(m+k,m)$ we have $k + m = 0 + m + k$ so that $(k,0) \sim (m+k, m)$ proving that $\sim[(k,0)] = \sim[(m+k,m)] \underset{\text{[eq: 7.5}}{=} z$, proving that $z \in \mathbb{Z}_0^+ \subseteq \mathbb{Z}_0^+ \bigcup \mathbb{Z}_0^-$.

From the above we have $\mathbb{Z} \subseteq \mathbb{Z}_0^+ \bigcup \mathbb{Z}_0^-$ which by [eq: 7.4] proves that

$$\mathbb{Z} = \mathbb{Z}_0^+ \bigcup \mathbb{Z}_0^-$$

As $0 = \sim[(0,0)] \in \mathbb{Z}_0^+$ and $0 = \sim[(0,0)] \in \mathbb{Z}_0^-$ we have that $\{0\} \in \mathbb{Z}_0^+ \bigcap \mathbb{Z}_0^-$. Let $z \in \mathbb{Z}_0^+ \bigcap \mathbb{Z}_0^-$ then there exists $n, m \in \mathbb{N}_0$ such that $z = \sim[(n,0)] = \sim[(0,m)]$ hence $n + 0 = 0 + m \Rightarrow n = m$,. So $z = \sim[(n, 0)] = \sim[(0,n)] = -z$. Applying then [theorem: 7.15] it follows that $z = 0$ or $\mathbb{Z}_0^+ \bigcap \mathbb{Z}_0^- \subseteq \{0\}$. Hence

$$\mathbb{Z}_0^+ \bigcap \mathbb{Z}_0^- = \{0\}$$ □

We can now define order relation on $\mathbb{Z}$.

Theorem 7.28. (Order relation in $\mathbb{Z}$) $\langle\mathbb{Z},\leqslant\rangle$ *where*

$$\leqslant=\{(n,m)\in\mathbb{Z}\times\mathbb{Z}|m+(-n)\in\mathbb{Z}_0^+|\}$$

is a totally ordered set.

Proof.

reflexivity. If $z\in\mathbb{Z}$ then $z+(-z)=0\in\mathbb{Z}_0^+$ so that $z\leqslant z$.

anti symmetry. Let $x,y\in\mathbb{Z}$ with $x\leqslant y$ and $y\leqslant x$ then

$$y+(-x)\in\mathbb{Z}_0^+\ \wedge\ x+(-y)\in\mathbb{Z}_0^+$$

then $\exists n,m\in\mathbb{N}_0$ such that

$$y+(-x)=\sim[(n.0)]\wedge x+(-y)=\sim[(m,0)]$$

so taking the sum we have

$$\begin{aligned}\sim[0,0] &= 0\\ &= y+(-x)+x+(-y)\\ &= \sim[(n,0)]+\sim[(m,0)]\\ &= \sim[(n+m,0)]\end{aligned}$$

Hence $0+0=0+n+m$ so that $n+m=0$ which by [theorem: 5.57] proves that $n=m=0$ so that $y+(-x)=\sim[(n,0)]=\sim[(0,0)]=0$. So $x=y+(-x)+x=0+x=x$.

transitivity. If $x\leqslant y$ and $y\leqslant z$ then $y+(-x)\in\mathbb{Z}_0^+$ and $z+(-y)\in\mathbb{Z}_0^+$. Using [theorem: 7.24] we have that $z+(-x)=(z+(-y))+(y+(-x))\in\mathbb{Z}_0^+$ so that $x\leqslant z$.

total ordering. If $x,y\in\mathbb{N}_0$ then we have for $x+(-y)\in\mathbb{Z}\underset{\text{[theorem: 7.27]}}{=}\mathbb{Z}_0^+\bigcup\mathbb{Z}_0^-$ the following:

$\boldsymbol{x+(-y)\in\mathbb{Z}_0^+}$**.** Then $y\leqslant x$

$\boldsymbol{x+(-y)\in\mathbb{Z}_0^-}$**.** Then $-(x+(-y))\in\mathbb{Z}_0^+$, as

$$\begin{aligned}-(x+(-y)) &\underset{\text{[theorem: 4.7]}}{=} -x+(-(-y))\\ &\underset{\text{[theorem: 4.8]}}{=} -x+y\\ &= y+(-x)\end{aligned}$$

proving that $x\leqslant y$. □

Using the order relation we have the following identity

Theorem 7.29. $\mathbb{Z}_0^+=\{x\in\mathbb{Z}|0\leqslant x\}$ *and* $\mathbb{Z}_0^-=\{x\in\mathbb{Z}|x\leqslant 0\}$

Proof. First we have

$$x+(-0)\underset{\text{[theorem: 4.8]}}{=}x+0=x \tag{7.7}$$

Now

$$\begin{aligned}x\in\mathbb{Z}_0^+ &\underset{\text{[eq: 7.7]}}{\Leftrightarrow} x+(-0)\in\mathbb{Z}_0^+\\ &\Leftrightarrow 0\leqslant x\\ &\Leftrightarrow x\in\{x\in\mathbb{Z}|0\leqslant x\}\end{aligned}$$

proving

$$\mathbb{Z}_0^+=\{x\in\mathbb{Z}|0\leqslant x\}$$

Further

$$\begin{array}{rcl} x\in\mathbb{Z}_0^- & \Leftrightarrow & -x\in\mathbb{Z}_0^+ \\ & \Leftrightarrow & 0+(-x)\in\mathbb{Z}_0^+ \\ & \Leftrightarrow & x\leqslant 0 \\ & \Leftrightarrow & x\in\{x\in\mathbb{Z}|x\leqslant 0\} \end{array}$$

proving

$$\mathbb{Z}_0^- = \{x\in\mathbb{Z}|x\leqslant 0\}$$

□

Theorem 7.30. *If $x,y\in\mathbb{Z}$ then we have*

1. $x\leqslant y\Leftrightarrow -y\leqslant -x$
2. $x<y\Leftrightarrow -y<-x$

Proof.

1.

⇒. If $x\leqslant y$ then $y+(-x)\in\mathbb{Z}_0^+$, further

$$\begin{array}{rcl} (-x)+(-(-y)) & \underset{[\text{theorem: } 4.8]}{=} & (-x)+y \\ & = & y+(-x) \\ & \in & \mathbb{Z}_0^+ \end{array}$$

proving that

$$-y\leqslant -x$$

⇐. If $-y\leqslant -x$ then we have by the above that $-(-x)\leqslant -(-y)\underset{[\text{theroem: } 4.8]}{\Rightarrow} x\leqslant y$

2.

$$\begin{array}{rcl} x<y & \Leftrightarrow & x\neq y\wedge x\leqslant y \\ & \Leftrightarrow & x\neq y\wedge -y\leqslant -x \\ & \underset{[\text{theorem: } 4.9]}{\Leftrightarrow} & -x\neq -y\wedge -y\leqslant -x \\ & \Leftrightarrow & -y<-x \end{array}$$

□

Theorem 7.31. *If $x\in\mathbb{Z}$ so that $x=\sim[(n,m)]$ then we have*

1. $0\leqslant x\Leftrightarrow m\leqslant n$
2. $0<x\Leftrightarrow m<n$
3. *If* $0<x$ *then* $1\leqslant x$

Proof.

1.

$$\begin{array}{rcl} 0\leqslant x & \underset{[\text{theorem: } 7.29]}{\Leftrightarrow} & x\in\mathbb{Z}_0^+ \\ & \Leftrightarrow & \exists k\in\mathbb{N}_0 \,\text{such that}\, x=\sim[(k,0)] \\ & \Leftrightarrow & \exists k\in\mathbb{N}_0 \text{ such that } n+0=m+k\Leftrightarrow n=m+k \\ & \underset{[\text{theorem: } 5.62]}{\Leftrightarrow} & m\leqslant n \end{array}$$

2. First

$$\begin{array}{rcl} x\neq 0 & \Leftrightarrow & \sim[(n,m)]\neq\sim[(0,0)] \\ & \Leftrightarrow & n+0\neq m+0 \\ & \Leftrightarrow & n\neq m \end{array}$$

then

$$\begin{aligned}0<x &\Leftrightarrow x\neq 0\wedge 0\leqslant x\\ &\Leftrightarrow n\neq m\wedge 0\leqslant x\\ &\underset{(1)}{\Leftrightarrow} n\neq m\wedge m\leqslant n\\ &\Leftrightarrow m<n\end{aligned}$$

3. If $0<x$ then by (2) $m<n$ so that by [theorem: 5.50]

$$m+1\leqslant n.$$

Now

$$x+(-1)=\sim[(n,m)]+\sim[(0,1)]=\sim[(n,m+1)]$$

so that $0\leqslant x+(-1)$, hence $x+(-1)\in\mathbb{Z}_0^+$ from which we conclude that

$$1\leqslant x$$

□

Theorem 7.32. *If $n,m,k\in\mathbb{Z}$ then*

1. $n\leqslant m\Leftrightarrow n+k\leqslant m+k$
2. $n<m\Leftrightarrow n+k<m+k$
3. $n\leqslant m\Leftrightarrow 0\leqslant m+(-n)$
4. $n<m\Leftrightarrow 0<m+(-n)$
5. $n<m\Leftrightarrow \exists k\in\mathbb{Z}_0^+\setminus\{0\}$ *such that* $m=k+n$
6. $n\leqslant m\Leftrightarrow \exists k\in\mathbb{Z}_0^+$ *such that* $m=\mathrm{kk}+n$.

Proof.

1.

$$\begin{aligned}n\leqslant m &\Leftrightarrow m+(-n)\in\mathbb{Z}_0^+\\ &\Leftrightarrow m+0+(-n)\in\mathbb{Z}_0^+\\ &\Leftrightarrow m+k+(-k)+(-n)\in\mathbb{Z}_0^+\\ &\underset{[\text{theorem: }4.7]}{\Leftrightarrow} (m+k)+(-(k+n))\in\mathbb{Z}_0^+\\ &\Leftrightarrow m+k+(-(n+k))\in\mathbb{Z}_0^+\\ &\Leftrightarrow n+k\leqslant m+k\end{aligned}$$

2.

$$\begin{aligned}n<m &\Leftrightarrow n\neq m\wedge n\leqslant m\\ &\Leftrightarrow n+k\neq m+k\wedge n\leqslant m\\ &\underset{(1)}{\Leftrightarrow} n+k\neq m+k\wedge n+k\leqslant m+k\\ &\Leftrightarrow n+k<m+k\end{aligned}$$

3.

$$\begin{aligned}n\leqslant m &\Leftrightarrow m+(-n)\in\mathbb{Z}_0^+\\ &\underset{[\text{theorem: }7.29}{\Leftrightarrow} 0\leqslant m+(-n)\end{aligned}$$

4.

$$\begin{aligned}n<m &\Leftrightarrow n\neq m\wedge n\leqslant m\\ &\underset{(3)}{\Leftrightarrow} n\neq m\wedge 0\leqslant m+(-n)\\ &\Leftrightarrow 0\neq m+(-n)\wedge 0\leqslant m+(-n)\\ &\Leftrightarrow 0<m+(-n)\end{aligned}$$

5.

⇒. Assume that $n<m$. Then by (2) we have that $0=n+(-n)<m+(-n)$, so if we take $k=m+(-n)$ we have that $0<k$ hence $k\in\mathbb{Z}_0^+\setminus\{0\}$. Further $n+k=(m+(-n))+n=m+((-n)+n)=m+0=m$. So we found a $k\in\mathbb{Z}_0^+\setminus\{0\}$ such that $m=n+k$.

⇐. If $k\in\mathbb{Z}_0^+\setminus\{0\}$ such that $m=n+k$ then as $0<k$ we have by (2)

$$n=0+n<k+n=n+k=m$$

so that

$$n<m$$

6.

⇒. Assume that $n\leqslant m$. Then by (1) we have that $0=n+(-n)\leqslant m+(-n)$, so if we take $k=m+(-n)$ we have that $0\leqslant k$ hence $k\in\mathbb{Z}_0^+$. Further $n+k=(m+(-n))+n=m+((-n)+n)=m+0=m$. So we found a $k\in\mathbb{Z}_0^+$ such that $m=n+k$.

⇐. If $k\in\mathbb{Z}_0^+$ such that $m=n+k$ then as $0\leqslant k$ we have by (1)

$$n=0+n\leqslant k+n=n+k=m$$

so that

$$n\leqslant m$$

□

Theorem 7.33. *If $x,y\in\mathbb{Z}$ and $0<x\wedge 0<y$ then $0<x\cdot y$*

Proof. If $x=\sim[(n.m)]$ and $y=\sim[(r,s)]$ then by [theorem: 7.31] we have $m<n$ and $s<r$ so by [theorem: 5.60] there exists $k,l\in\mathbb{N}_0\setminus\{0\}$ such that $n=m+k$ and $r=s+l$. Hence

$$\begin{aligned}
n\cdot r+m\cdot s &= (m+k)\cdot(s+l)+m\cdot s\\
&= \underbrace{m\cdot s}_{1}+\underbrace{m\cdot l}_{2}+\underbrace{k\cdot s}_{3}+k\cdot l+\underbrace{m\cdot s}_{4}\\
m\cdot r+n\cdot s &= m\cdot(s+l)+(m+k)\cdot s\\
&= \underbrace{m\cdot s}_{1}+\underbrace{m\cdot l}_{2}+\underbrace{m\cdot s}_{4}+\underbrace{k\cdot s}_{3}
\end{aligned}$$

so that

$$n\cdot r+m\cdot s=m\cdot r+n\cdot s+k\cdot l$$

As $0\neq k$ and $0\neq l$ it follows from [theorem: 5.75] that $k\cdot l\neq 0$, using the above together with [theorem: 5.61] proves that

$$m\cdot r+n\cdot s<n\cdot r+m\cdot s \tag{7.8}$$

now

$$x\cdot y \;=\; \sim[(n\cdot r+m\cdot s, m\cdot r+n\cdot s)]$$

Combining the above with [eq: 7.8] and [theorem: 7.31 proves finally:

$$0<x\cdot y$$

□

Theorem 7.34. *If $n,m,k\in\mathbb{Z}$ then we have:*

1. *If $0<k$ then $n<m\Leftrightarrow n\cdot k<m\cdot k$*
2. *If $k<0$ and $n<m\Leftrightarrow m\cdot k<n\cdot k$*
3. *If $0\leqslant k$ and $n\leqslant m$ then $n\cdot k\leqslant m\cdot k$*
4. *If $k\leqslant 0$ and $n\leqslant m$ then $m\cdot k\leqslant n\cdot k$*

Proof.

1.

⇒. From $n<m$ we have by [theorem: 7.32] that $0<m+(-n)$, so using the previous theorem [theorem: 7.33] it follows that

$$\begin{array}{rcl} 0 & < & (m+(-n))\cdot k \\ & = & m\cdot k+(-n)\cdot k \\ & = & m\cdot k+(-1)\cdot n\cdot k \\ & = & m\cdot k+(-(n\cdot k)) \end{array}$$

which by [theorem: 7.32] proves that $n\cdot k<m\cdot k$. Hence we have proved that

$$n<m\Rightarrow n\cdot k<m\cdot k \tag{7.9}$$

⇐. Let $n\cdot k<m\cdot k$, if $n=m$ then we would reach the contradiction that $n\cdot k=m\cdot k$, so we have either $n<m$ or $m<n$. If $m<n$ then from [eq: 7.9] we have $m\cdot k<n\cdot k$ leaving to the contradiction $n\cdot k<n\cdot k$, so we must have that $n<m$. Hebce

$$n\cdot k<m\cdot k\Rightarrow n<m$$

2.

⇒. Let $n<m$. As $k<0$ we have by [theorem: 7.30] $-0<(-k)\underset{\text{[theorem: 4.8]}}{\Rightarrow}0<-k$. So we have by (1) that

$$n\cdot(-k)<m\cdot(-k)$$

Using [theorem: 7.18] we have that $-(n\cdot k)=n\cdot(-k)$ and $-(m\cdot k)=m\cdot(-k)$ so that by the above we have $-(n\cdot k)<-(m\cdot k)$. Applying then [theorem: 7.30] we have $m\cdot k<n\cdot k$. So

$$n<m\Rightarrow m\cdot k<n\cdot k$$

⇐. Let $m\cdot k<n\cdot k$. Using [theorem: 7.30] we have that $m\cdot-(n\cdot k)<-(m\cdot k)$ giving by [theorem: 7.18] that

$$n\cdot(-k)<m\cdot(-k) \tag{7.10}$$

As $k<0$ we have by [theorem: 7.30] $-0<(-k)\underset{\text{[theorem: 4.8]}}{\Rightarrow}0<-k$, so applying (1) on [eq: 7.10] gives $n<m$, hence we have proved that

$$m\cdot k<n\cdot k\Rightarrow n\cdot m$$

3. For k we have the following possibilities:

$k=0$. Then $n\cdot k=n\cdot 0=0=m\cdot 0=m\cdot k$ so that $n\cdot k\leqslant m\cdot k$.

$0<k$. For $n\leqslant m$ we have either:

$n=m$. Then $n\cdot k=m\cdot k$ so that $n\cdot k\leqslant m\cdot k$

$n<m$. Then using (1) $n\cdot k<m\cdot k$ so that $n\cdot k\leqslant m\cdot k$

4. For k we have the following possibilities:

$k=0$. **$k=0$.** Then $n\cdot k=n\cdot 0=0=m\cdot 0=m\cdot k$ so that $m\cdot k\leqslant n\cdot k$.

$k<0$. For $n\leqslant m$ we have either:

$n=m$. Then $n\cdot k=m\cdot k$ so that $m\cdot k\leqslant n\cdot k$.

$n<m$. Then using (2) we have that $m\cdot k<n\cdot k$

□

Corollary 7.35. *If* $x\in\mathbb{Z}$ *then* $0\leqslant x\cdot x$

Proof. As $x \in \mathbb{Z} \underset{[\text{theorem: } 7.27]}{=} \mathbb{Z}_0^+ \bigcup \mathbb{Z}_0^-$ we have the folowing cases to consider:

$\boldsymbol{x \in \mathbb{Z}_0^+}$**.** Then $0 \leqslant x$ so that by [corollary: 7.34] $0 = 0 \cdot x \leqslant x \cdot x$.

$\boldsymbol{x \in \mathbb{Z}_0^-}$**.** Then $-x \in \mathbb{Z}_0^+$ so that

$$0 \leqslant (-x) \cdot (-x)$$

Now $x \cdot x = \sim[(n, m)] \cdot \sim[(n, m)] = \sim[(n \cdot n + m \cdot m, m \cdot n + n \cdot m)]$ so that $0 \leqslant x \cdot x$. □

Theorem 7.36. *$i_{\mathbb{N}_0}: \mathbb{N}_0 \rightarrow \mathbb{Z}_0^+$ defined by $i_{\mathbb{N}_0}(n) = \sim[(n, 0)]$ is a order isomorphism between $\langle N_0, \leqslant\rangle$ and $\langle \mathbb{Z}_0^+, \leqslant\rangle$. In other words $i_{\mathbb{N}_0}: \mathbb{N}_0 \rightarrow \mathbb{Z}_0^+$ is a bijection and $x \leqslant y \Leftrightarrow i_{\mathbb{N}_0}(x) \leqslant i_{\mathbb{N}_0}(y)$.*

Proof. Using [theorem: 7.24] it follows that

$$i_{\mathbb{N}_0}: \mathbb{N}_0 \rightarrow \mathbb{Z}_0^+ \text{ is a bijection}$$

Further we have:

$$\begin{array}{rcl} i_{\mathbb{N}_0}(x) \leqslant i_{\mathbb{N}_0}(y) & \Leftrightarrow & i_{\mathbb{N}_0}(y) + (-i_{\mathbb{N}_0}(x)) \in \mathbb{Z}_0^+ \\ & \Leftrightarrow & \sim[(y, 0)] + (-[(x, 0)]) \in \mathbb{Z}_0^+ \\ & \Leftrightarrow & \sim[(y, 0)] + \sim[(0, x)] \in \mathbb{Z}_0^+ \\ & \Leftrightarrow & \sim[(y, x)] \in \mathbb{Z}_0^+ \\ & \underset{[\text{theorem: } 7.31]}{\Leftrightarrow} & x \leqslant y \end{array}$$

□

The above theorem allows us to transfer properties of $\mathbb{N}_0$ to $\mathbb{Z}_0^+$ as is expressed in the following theorems.

Theorem 7.37. (Archimedean property) *If $x, y \in \mathbb{Z}$ with $0 < x$ then there exist a $k \in \mathbb{Z}_0^+$such that $y < k \cdot x$*

Proof. We have the following cases for x:

$\boldsymbol{x \leqslant 0}$**.** Take $k = 1 \in \mathbb{Z}_0^+$ then as $x \leqslant 0 < y = 1 \cdot y = k \cdot y$ proving that $x < k \cdot y$

$\boldsymbol{0 < x}$**.** Then $x \in \mathbb{Z}_0^+$ so that as $i_{\mathbb{N}_0}: \mathbb{N}_0 \rightarrow \mathbb{Z}_0^+$ defined by $i_{\mathbb{N}_0}(n) = \sim[(n, 0)]$ is a group isomorphism [see theorem: 7.24] between $\langle \mathbb{N}_0, +\rangle$ and $\langle \mathbb{Z}_0^+, +\rangle$. Take $n = (i_{\mathbb{N}_0})^{-1}(x)$ and $m = (i_{\mathbb{N}_0})^{-1}(y)$ then $x = i_{\mathbb{N}_0}(n)$ and $n \neq 0$ [otherwise $x = i_{\mathbb{N}_0}(n) = i_{\mathbb{N}_0}(0) = 0$]. Using the Archimedean property of the natural numbers [see theorem: 5.77] there exists a $l \in \mathbb{N}_0$ such that $m < l \cdot n$. So by [theorem: 7.36] we have that

$$i_{\mathbb{N}_0}(m) < i_{\mathbb{N}_0}(l \cdot n) \underset{[\text{theorem: } 7.24]}{=} i_{\mathbb{N}_0}(l) \cdot i_{\mathbb{N}_0}(n) \tag{7.11}$$

Take $k = i_{\mathbb{N}_0}(l) \in \mathbb{Z}_9^+$ then as $i_{\mathbb{N}_0}(n) = i_{\mathbb{N}_0}((i_{\mathbb{N}_0})^{-1}(x)) = x$ and $i_{\mathbb{N}_0}(m) = i_{\mathbb{N}_0}((i_{\mathbb{N}_0})^{-1}(y)) = y$ we have by [eq: 7.11] that

$$y < k \cdot x$$

□

Theorem 7.38. *$\langle \mathbb{Z}_0^+, \leqslant\rangle$ is a well-ordered set*

Proof. Using [theorem: 7.36] we have that

$$i_{\mathbb{N}_0}: \mathbb{N}_0 \rightarrow \mathbb{Z}_0^+ \text{ is a order isomorphism between } \langle \mathbb{N}_0, \leqslant\rangle \text{ and } \langle \mathbb{Z}_0^+\rangle$$

Let $A \subseteq \mathbb{Z}_0^+$ such that $A \neq 0$ then as $i_{\mathbb{N}_0}$ is a bijection, hence a surjection, we have that $(i_{\mathbb{N}_0})^{-1}(A) \neq \varnothing$. By [theorem: 5.51] $\langle \mathbb{N}_0, \leqslant\rangle$ is well-ordered so there exists a least element m of $(i_{\mathbb{N}_0})^{-1}(A)$. So

$$m \in (i_{\mathbb{N}_0})^{-1}(A) \text{ and } \forall n \in (i_{\mathbb{N}_0})^{-1}(A) \text{ we have } m \leqslant n$$

As $m \in (i_{\mathbb{N}_0})^{-1}(A)$ we have for $M = i_{\mathbb{N}_0}(m)$ that

$$M \in A \tag{7.12}$$

Further if $x \in A$ then as $i_{\mathbb{N}_0}((i_{\mathbb{N}_0})^{-1}(x)) = x \in A$ we have that $(i_{\mathbb{N}_0})^{-1}(x) \in (i_{\mathbb{N}_0})^{-1}(A)$ so that $m \leqslant (i_{\mathbb{N}_0})^{-1}(x)$, hence by [theorem: 7.36] we have that $M = i_{\mathbb{N}_0}(m) \leqslant i_{\mathbb{N}_0}((i_{\mathbb{N}_0})^{-1}(x)) = x$. Proving that

$$\forall x \in A \text{ we have } M \leqslant x \tag{7.13}$$

From [eq: 7.12] and [eq: 7.13] it follows that A has a least element proving that $\langle \mathbb{Z}_0^+, \leqslant \rangle$ is a well-ordered set. □

Theorem 7.39. *$\langle \mathbb{Z}_0^+, \leqslant \rangle$ is conditional complete [see definition: 3.73].*

Proof. As by [theorem: 7.38] $\langle \mathbb{Z}_0^+, \leqslant \rangle$ is well-ordered it follows from [theorem: 3.79] it follows that $\langle \mathbb{Z}_0^+, \leqslant \rangle$ is conditional complete. □

Theorem 7.40. *If $A \subseteq \mathbb{Z}_0^+$ is such that $A \neq \varnothing$ and $\sup(A)$ exists then $\sup(A) \in A$.*

Proof. By [theorem: 7.36]

$$i_{\mathbb{N}_0}: \mathbb{N}_0 \rightarrow \mathbb{Z}_0^+ \text{ is a order isomorphism between } \langle \mathbb{N}_0, \leqslant \rangle \text{ and } \langle \mathbb{Z}_0^+, \leqslant \rangle$$

which by [theorem: 3.53] means that

$$(i_{\mathbb{N}_0})^{-1}: \mathbb{Z}^+ \rightarrow \mathbb{N}_0 \text{ is a order isomorphism between } \langle \mathbb{Z}_0^+, \leqslant \rangle \text{ and } \langle \mathbb{N}_0, \leqslant \rangle$$

Assume that $M = \sup(A)$ exists then by [theorem: 3.75] $\sup((i_{\mathbb{N}_0})^{-1}(A))$ exist and $\sup((i_{\mathbb{N}_0})^{-1}(A)) = (i_{\mathbb{N}_0})^{-1}(M)$. By [theorem: 5.72] we have that $\sup((i_{\mathbb{N}_0})^{-1}(A)) \in (i_{\mathbb{N}_0})^{-1}(A)$ so that $(i_{\mathbb{N}_0})^{-1}(M) \in (i_{\mathbb{N}_0})^{-1}(A)$, hence $M = i_{\mathbb{N}_0}((i_{\mathbb{N}_0})^{-1}(M)) \in (i_{\mathbb{N}_0})((i_{\mathbb{N}_0})^{-1}(A)) = A$ or

$$\sup(A) \in A$$

□

Definition 7.41. (Absolute Value) *If $x \in \mathbb{Z}$ then $|x|$ is defined by*

$$|x| = \begin{cases} x & \text{if } 0 \leqslant x \\ -x & \text{if } x < 0 \end{cases}$$

Theorem 7.42. *If $x, y \in \mathbb{Z}$ then $|x \cdot y| = |x| \cdot |y|$*

Proof. We have the following possibilities for x, y:

$\mathbf{0 \leqslant x \wedge 0 \leqslant y}$**.** Then $|x| = x$ and $|y| = y$. Further by [theorem: 7.34] $0 = 0 \cdot y \leqslant x \cdot y$, hence $x \cdot y = |x \cdot y|$. So we have that $|x \cdot y| = |x| \cdot |y|$.

$\mathbf{0 \leqslant x \wedge y < 0}$**.** Then $x = |x|$ and $-y = |y|$, further by [theorem: 7.34] $x \cdot y \leqslant 0 \cdot y = 0$, hence $|x \cdot y| = -(x \cdot y)$. So

$$|x| \cdot |y| = x \cdot (-y) \underset{\text{[theorem: 7.18]}}{=} -(x \cdot y) = |x \cdot y|.$$

$\mathbf{x < 0 \wedge 0 \leqslant y}$**.** Then $-x = |x|$ and $y = |y|$, further by [theorem: 7.34] $x \cdot y = y \cdot x \leqslant 0 \cdot x = 0$, hence $|x \cdot y| = -(x \cdot y)$. So

$$|x| \cdot |y| = (-x) \cdot y \underset{\text{[theorem: 7.18]}}{=} -(x, y) = |x \cdot y|$$

$\mathbf{x < 0 \wedge y < 0}$**.** Then $-x = |x|$, $-y = |y|$, further by [theorem: 7.34] $0 = 0 \cdot y < x \cdot y$, hence $|x \cdot y| = x \cdot y$. So

$$|x| \cdot |y| = (-x) \cdot (-y) \underset{\text{[theorem: 7.18]}}{=} -(x \cdot (-y)) \underset{\text{[theorem: 7.18]}}{=} -(-(x \cdot y)) = x \cdot y \underset{\text{[theorem: 4.8]}}{=} |x \cdot y|$$

□

Theorem 7.43. *If $x \in \mathbb{Z}$ then $x \leqslant |x|$*

Proof. If $0 \leqslant x$ then $x = |x|$ so that trvially $x \leqslant |x|$, if $x < 0$ then by [theorem: 7.31] $0 < -x = |x|$ so that by transitivity $x < |x|$ or $x \leqslant |x|$. □

We introduce now division, just as was done for the natural numbers.

Theorem 7.44. (Division Algorithm) *If $n, m \in \mathbb{Z}$ and $0 < n$ then there exists **unique** $r \in \mathbb{Z}_0^+$, $q \in \mathbb{Z}$ such that $0 \leqslant r < n$ and $m = n \cdot q + r$*

Proof. First we prove existence, let $m, n \in \mathbb{Z}$ with $0 < n$. Define

$$A_{n,m} = \{m + n \cdot q | q \in \mathbb{Z} \wedge 0 \leqslant m + n \cdot q\} \subseteq \mathbb{Z}_0^+.$$

Using the Archimedean property of $\mathbb{Z}$ [see theorem: 7.37] there exist a $k \in \mathbb{Z}_0^+$ such that $-m < n \cdot k$, using [theorem: 7.32] it follows that $0 \leqslant n \cdot k + (-(-m)) = n \cdot k + m = m + n \cdot k$ proving that $m + n \cdot k \in A_{n,m}$, hence $A_{n,m} \neq \varnothing$. As $\langle \mathbb{Z}_0^+, \leqslant \rangle$ is well-ordered [see theroem: 7.38] $A_{n,m}$ has a least element, hence

$$\exists r' \in A_{n,m} \text{ such that } \forall a \in A_{n,m} \text{ we have } r' \leqslant a \tag{7.14}$$

As $r' \in A_{n,m}$ there exist a $q' \in \mathbb{Z}$ such that

$$r' = m + n \cdot q' \text{ and } 0 \leqslant r' \tag{7.15}$$

Assume that $n < r'$ then by [theorem: 7.32] $\exists k \subset \mathbb{Z}_0^+ \setminus \{0\}$ such that $r' = n + k$. Hence $m + n \cdot q' = n + k$ so that $0 < k = m + n \cdot q' + (-n) = m + (q' - 1) \cdot n$ proving that $k \in A_{n,m}$. Now $0 < n \underset{\text{[theorem: 7.32]}}{\Rightarrow} k < n + k = r' \Rightarrow k < r'$, as $k \in A_{n,m}$ we have by [eq: 7.14] $r' \leqslant k$, giving the contradiction $k < k$. So we must have that $r' \leqslant n$ or

r' = n. In this case we we have that $m + n \cdot q' = r' = n$, hence

$$m = n + (-(n \cdot q')) = n \cdot 1 + n \cdot (-q') = n \cdot (1 + (-q'))$$

So taking $q = (1 + (-q'))$ and $r = 0 < n$ then

$$m = n \cdot q + r \text{ and } 0 \leqslant r < n$$

r' < n. Then as $r' = m + n \cdot q'$ we have $m = r' + (-(n \cdot q')) = r' + n \cdot (-q')$, so taking $q = -q'$ and $r = r'$ then

$$m = n \cdot q + r \text{ and } 0 \leqslant r' < n$$

Now for uniqueness assume that there exists $q_1, q_2 \in \mathbb{Z}$ and $r_1, r_2 \in \mathbb{Z}_0^+$ such that

$$m = n \cdot q_1 + r_1 \wedge m = n \cdot q_2 + r_2 \wedge 0 \leqslant r_1 < n \wedge 0 \leqslant r_2 < n$$

Then

$$\begin{aligned} n \cdot q_1 + r_1 = n \cdot q_2 + r_2 &\Rightarrow n \cdot q_1 + (-(n \cdot q_2)) = r_2 + (-r_1) \\ &\Rightarrow n \cdot (q_1 + (-q_2)) = r_2 + (-r_1) && (7.16) \\ n \cdot q_1 + r_1 = n \cdot q_2 + r_2 &\Rightarrow n \cdot q_2 + (-(n \cdot q_1)) = r_1 + (-r_2) \\ &\Rightarrow n \cdot (q_2 + (-q_1)) = r_1 + (-r_2) && (7.17) \end{aligned}$$

Assume now that $r_1 \neq r_2$ then we have either:

r₁ < r₂. Then by [theorem: 7.32] $0 < r_2 + (-r_1) \underset{\text{[eq: 7.16]}}{=} n \cdot (q_1 + (-q_2))$, hence $0 \cdot k < n \cdot (q_1 + (-q_2))$ as $0 < n$ we must have by [theorem: 7.34] that $0 < q_1 + (-q_2)$. Using [theorem: 7.31] we have

$$1 \leqslant q_1 + (-q_2) \tag{7.18}$$

As $r_2 < n$ we have by [theorem: 7.32] that $r_2 + (-r_1) < n + (-r_1)$, further as $(-r_1) \leqslant 0$ we have by [theorem: 7.32] that $n + (-r_1) \leqslant n$ so that $r_2 + (-r_1) < n$. Using this with [eq: 7.16] gives $n \cdot (q_1 + (-q_2)) < n = 1 \cdot n$, hence using [theorem: 7.34] we have that $q_2 + (-q_1) < 1$, contradicting [eq: 7.18]. So this case never occurs.

r₂ < r₁. Then by [theorem: 7.32] $0 < r_1 + (-r_2) \underset{\text{[eq: 7.17]}}{=} n \cdot (q_2 + (-q_1))$, hence $0 \cdot k < n \cdot (q_2 + (-q_1))$ as $0 < n$ we must have by [theorem: 7.34] that $0 < q_2 + (-q_1)$. Using [theorem: 7.31] we have

$$1 \leqslant q_2 + (-q_1) \tag{7.19}$$

As $r_1 < n$ we have by [theorem: 7.32] that $r_1 + (-r_2) < n + (-r_2)$, further as $(-r_2) \leqslant 0$ we have by [theorem: 7.32] that $n + (-r_2) \leqslant n$ so that $r_1 + (-r_2) < n$. Using this with [eq: 7.17] gives $n \cdot (q_2 + (-q_1)) < n = 1 \cdot n$, hence using [theorem: 7.34] we have that $q_1 + (-q_2) < 1$, contradicting [eq: 7.19]. So this case never occurs.

As all the cases lead to a contradiction the assumption $r_1 \neq r_2$ is wrong. Hence

$$r_1 = r_2$$

So $n \cdot q_1 + r_1 \underset{r_1 = r_2}{=} n \cdot q_2 + r_1$ giving by adding $-r_1$ to both sides that $n \cdot q_1 = n \cdot q_2$. Applying [theorem: 7.19] proves then

$$q_1 = q_2$$ □

Definition 7.45. *If $n, m \in \mathbb{Z}$ then we say that n divides m noted as $n|m$ if there exist a $q \in \mathbb{Z}$ such that $q \cdot n = m$, we call n a **divisor** of m.*

Example 7.46. Every integer is a divisor of 0.

Proof. If $n \in \mathbb{Z}$ then $n \cdot 0 = 0$ □

Example 7.47. If $n \in \mathbb{Z}$ then $1|n$

Proof. As $1 \cdot n = n$ we have by definition $1|n$. □

Theorem 7.48. *Let $m \in \mathbb{Z}$ then if $n|m$ we have that $(-n)|m$. In other words if n is a divisor of m then $-n$ is a divisor of m.*

Proof. If $n|m$ then there exist a q such that $n \cdot q = m$, then $(-n) \cdot (-q) = n \cdot q = m$ so that $(-n)|m$. □

Theorem 7.49. *If $m \in \mathbb{Z}$ and $n \in \mathbb{Z} \setminus \{0\}$ a divisor of m then there exists a **unique** q such that $n \cdot q = m$*

Proof. Existence follows from the definition of divisor. Now for uniqueness assume that $q_1, q_2 \in \mathbb{Z}$ such that $n \cdot q_1 = m = n \cdot q_2$ then by [theorem: 7.19] $q_1 = q_1$. □

Definition 7.50. *If $m \in \mathbb{Z}$ and $n \in \mathbb{Z} \setminus \{0\}$ then the unique number q such that $m = n \cdot q$ is called the **quotient** of n and m and is noted as $\frac{m}{n}$. So $n \cdot \frac{m}{n} = m$.*

Definition 7.51. **(Common Divisor)** *If $n, m \in \mathbb{Z}$ then d is a **common divisor** of n and m if $d|n$ and $d|m$.*

Lemma 7.52. *If $n, m \in \mathbb{Z}$ such that $m \neq 0$ and $n|m$ then $n \leqslant |m|$*

Proof. As $n|m$ there exist a $q \in \mathbb{Z}$ such that $n \cdot q = m$, as $m \neq 0$ we must have $q \neq 0$ [otherwise $m = n \cdot q = 0$]. For n, m we have now the following possibilities to consider:

$\boldsymbol{0 < m \wedge n \leqslant 0}$. In this case we have $n \leqslant 0 < m \leqslant |m|$ so that $n \leqslant |m|$

$\boldsymbol{0 < m \wedge 0 < n}$. If $q \leqslant 0 \underset{q \neq 0}{\Rightarrow} q < 0 \underset{0 < n \wedge [\text{theorem: } 7.34]}{\Rightarrow} q \cdot n < n \cdot 0 = 0$ so that $m < 0$ contradicting $0 < m$, hence we must have that $0 < q$. Using [theorem: 7.31] we have $1 \leqslant q$ so that by [theorem: 7.34] $n = 1 \cdot n \leqslant q \cdot n = m = |m|$, hence $n \leqslant |m|$.

$\boldsymbol{m < 0 \wedge n \leqslant 0}$. Then $0 < -m = |m|$ so that $n \leqslant 0 < |m|$ giving $n \leqslant |m|$.

$\boldsymbol{m < 0 \wedge 0 < n}$. If $0 \leqslant q \underset{q \neq 0}{\Rightarrow} 0 < q \underset{0 < n \wedge [\text{theorem: } 7.34]}{\Rightarrow} 0 = 0 \cdot n < q \cdot n = m$ contradicting $m < 0$, hence $q < 0$. hence $0 < -q$. Using [theorem: 7.31] we have then

$$1 \leqslant -q \underset{[\text{theorem: } 7.34]}{\Rightarrow} n = n \cdot 1 \leqslant (-q) \cdot n = -(q \cdot n) = |m|$$

proving that $n \leqslant |m|$.

So in all cases we have

$$n \leqslant |m| \qquad \square$$

Theorem 7.53. *Let $n, m \in \mathbb{Z}$ with $n \neq 0$ then* $\max(\{d \in \mathbb{Z}_0^+ | d \textit{ is a common divisor of } n \textit{ and } m\})$ *exist.*

Proof. Let $n, m \in \mathbb{Z}$ and define $D_{n,m} = \{d \in \mathbb{Z}_0^+ | d \text{ is a common divisor of } n \text{ and } m\}$. By [example: 7.47] $0 < 1$ is a common divisor of n and m, which as $0 < 1$ means that $1 \in A_{n,m}$ so that $D_{n,m} \neq \varnothing$. Let $d \in D_{n,m}$ then as $d|n$ and $n \neq 0$ we have by [lemma: 7.52] that $d \leqslant |n|$ so that $D_{n,m}$ has a upper bound. As $\langle \mathbb{Z}_0^+, \leqslant \rangle$ is well ordered [see theorem: 7.38] it follows that $\max(D_{n,m})$ exist. $\square$

The above theorem ensures that the following defiition is well defined,

Definition 7.54. *Let $n, m \in \mathbb{Z}_0^+$ with $n \neq 0$ then*

$$\gcd(n, m) = \max(\{d \in \mathbb{Z}_0^+ | d \textit{ is a common divisor if } n \textit{ and } m\})$$

Definition 7.55. *A $z \in \mathbb{Z}$ is* ***even*** *if $2|z$ and* ***odd*** *is z is not even.*

Theorem 7.56. *Let $z \in \mathbb{Z}$ then we have*

1. *z is even $\Leftrightarrow \exists m \in \mathbb{Z}$ such that $z = 2 \cdot m$*
2. *z is oddd $\Leftrightarrow \exists m \in \mathbb{Z}$ such that $z = 2 \cdot m + 1$*

Proof.

1.
$$\begin{aligned} z \text{ is even} &\Leftrightarrow 2|z \\ &\Leftrightarrow \exists m \in \mathbb{Z} \text{ such that } z = 2 \cdot m \end{aligned}$$

2. Using the Division Algorithm [see: theorem: 7.44] there exists unique $q, r \in \mathbb{Z}$ such that $z = 2 \cdot q + r$ and $0 \leqslant r < 2$ s that $r \in \{0, 1\}$. So

$$\begin{aligned} z \text{ is odd} &\Leftrightarrow z \text{ is not even} \\ &\underset{r=0 \Rightarrow z \text{ is evn}}{\Leftrightarrow} z = 2 \cdot g + 1 \end{aligned}$$
$\square$

Theorem 7.57. *If $z \in \mathbb{Z}$ then we have*

1. *z is even $\Leftrightarrow z^2 = z \cdot z$ is even*
2. *z is odd $\Leftrightarrow z^2 = z \cdot z$ is odd*

Proof.

1. If z is even then $z = 2 \cdot m$ so that $z \cdot z = (2 \cdot m) \cdot (2 \cdot m) = 2 \cdot (2 \cdot (m \cdot m))$ proving that $z \cdot z$ is even. If $z.z$ is even then if z is odd we have $z = 2 \cdot m + 1$ so that

$$\begin{aligned} z \cdot z &= (2 \cdot m + 1) \cdot (2 \cdot m + 1) \\ &= 2 \cdot (m \cdot (2 \cdot m + 1)) + 2 \cdot m + 1 \\ &= 2 \cdot (m \cdot (2 \cdot m + 1) + m) + 1 \end{aligned}$$

proving that $z \cdot z$ is odd contradiction the fact that $z \cdot z$ is even, hence z should be even.

2. This follows from (1) by controposition. $\square$

7.3 Denumerability of the Integers

Theorem 7.58. $\mathbb{Z}_0^+$, $\mathbb{Z}_0^+$ *and $\mathbb{Z}$ are all denumerable*

Proof. Using [theorm: 7.24 (3)] there exists a bijection $i_{\mathbb{N}_0}: \mathbb{N}_0 \rightarrow \mathbb{Z}_0^+$ so that $\mathbb{N}_0 \approx \mathbb{Z}_0^+$

$$\mathbb{Z}_0^+ \text{ is denumerbable}$$

Define now $\beta: \mathbb{Z}_0^+ \rightarrow \mathbb{Z}_0^-$ then we have

injectivity. If $\beta(n) = \beta(n')$ then $-n = -n' \Rightarrow n = (-(-n)) = (-(-n')) = n'$

surjectivity. If $n \in \mathbb{Z}_0^- = \{-n | n \in \mathbb{Z}_0^-\}$ there exists $m \in \mathbb{Z}^+$ such that $n = -m = \beta(m)$

hence $\beta: \mathbb{Z}_0^+ - < \mathbb{Z}_0^-$ is a bijection proving that $\mathbb{Z}_0^+ \approx \mathbb{Z}_0^-$. So using [theorem: 6.24] it follows that

$$\mathbb{Z}_0^- \text{ is denumerable}$$

Finally as $\mathbb{Z} \underset{[\text{theorem: } 7.27]}{=} \mathbb{Z}_0^+ \bigcup \mathbb{Z}_0^-$ so that by [theorem: 6.61] we have

$$\mathbb{Z} \text{ is denumerable}$$

□

Chapter 8
The Rational Numbers

The reason to introduce the integer numbers was to extend it to the group $\langle \mathbb{Z}, + \rangle$ where $\mathbb{N}_0$ is in embeedded as $\mathbb{Z}_0^+$. For that we introduced a equivalence relation allowing us to have a additive inverse element. We introduced also mulltiplication making $\langle \mathbb{Z}, +, - \rangle$ a integral domain. Next we want to extend $\mathbb{Z}$ itself to a ring, again we will use equivalence relations to do this.

As was the case for $\mathbb{Z}$ we will have many common symbols where context must determine what the real meaning is of these at=ymbola.

Table of contents

Index