The HLM Proof Assistant

Library

Contents

Chapter 1

Essentials

1.1 Sets

Definition 1.1.1.

$$\varnothing := \{\}$$

Proposition 1.1.2. Let S be a set. Then:

$$\varnothing \subseteq S$$

Proof. Let $x \in \varnothing$. Then $x \in S$:

$$\begin{aligned} & x \in \varnothing \\ \overset{\text{def}}{\Rightarrow}\ & \text{false} \end{aligned}$$

□

Definition 1.1.3. Let S be a set. We define:

$$\begin{aligned} S \text{ is empty } :\Leftrightarrow\ & S = \varnothing \\ \Leftrightarrow\ & S \subseteq \varnothing \\ \Leftrightarrow\ & \nexists x \in S \end{aligned}$$

- Assume $S = \varnothing$.
  $$\overset{\text{def}}{\Rightarrow}\ S \subseteq \varnothing$$
- Assume $S \subseteq \varnothing$. Then $\nexists x \in S$:
  Assume $\exists x \in S$.
  $$\begin{aligned} & S \subseteq \varnothing \\ \overset{\text{def}}{\Rightarrow}\ & \forall s \in S\colon\ s \in \varnothing \\ \underset{s:=x}{\Rightarrow}\ & x \in \varnothing \\ \overset{\text{def}}{\Rightarrow}\ & \text{false} \end{aligned}$$
- Assume $\nexists x \in S$. Then $S = \varnothing$:

  $\subseteq$: $S \subseteq \varnothing$: Let $a \in S$. Then $a \in \varnothing$:

  $\exists x \in S$:

  Choose $x := a$.

$\supseteq$: $\varnothing \subseteq S$:

1.1.2 $\Rightarrow \varnothing \subseteq S$

Definition 1.1.4. Let S be a set. We define:

$$\begin{aligned} S \text{ is finite } &:\Leftrightarrow |S| \in \mathbb{N} \\ &\Leftrightarrow |S| < |\mathbb{N}| \\ &\Leftrightarrow \exists\, k \in \mathbb{N},\ f : S \leftrightarrow \mathbb{N}_{<k} \\ &\Leftrightarrow \exists\, l \in \mathbb{N},\ g : \mathbb{N}_{<l} \leftrightarrow S \\ &\Leftrightarrow \exists\, m \in \mathbb{N},\ h : S \to \mathbb{N}_{<m} :\ h \text{ is injective} \\ &\Leftrightarrow \exists\, n \in \mathbb{N},\ i : S \to \mathbb{N}_{\leq n} :\ i \text{ is injective} \\ &\Leftrightarrow \exists\, x \in \mathbb{N} :\ |S| \leq x \\ &\Leftrightarrow \exists\, y \in \mathbb{N} :\ |S| < y \end{aligned}$$

- Assume $|S| \in \mathbb{N}$. Then $\exists\, k \in \mathbb{N},\ f : S \leftrightarrow \mathbb{N}_{<k}$:

  1.4.2.2 $\Rightarrow |S| = |\mathbb{N}_{<|S|}|$

  $\overset{\text{def}}{\Rightarrow}\ \exists\, r : S \leftrightarrow \mathbb{N}_{<|S|}$

  Choose $k := |S|,\ f := r$.

- Assume $\exists\, k \in \mathbb{N},\ f : S \leftrightarrow \mathbb{N}_{<k}$. Then $\exists\, l \in \mathbb{N},\ g : \mathbb{N}_{<l} \leftrightarrow S$:

  Choose $l := k,\ g := f^{-1}$.

- Assume $\exists\, l \in \mathbb{N},\ g : \mathbb{N}_{<l} \leftrightarrow S$.

  $|\mathbb{N}_{<l}| = |S|$:

  $\exists\, s : S \leftrightarrow \mathbb{N}_{<l}$:

  Choose $s := g$.

  $\underset{l = |\mathbb{N}_{<l}|}{\overset{1.4.2.2}{\Rightarrow}}\ l = |S|$

  $l \in \mathbb{N}$

  $\underset{l = |S|}{\Rightarrow}\ |S| \in \mathbb{N}$

- Assume $\exists\, k \in \mathbb{N},\ f : S \leftrightarrow \mathbb{N}_{<k}$. Then $\exists\, m \in \mathbb{N},\ h : S \to \mathbb{N}_{<m} :\ h$ is injective:

  $\overset{\text{def}}{\Rightarrow}\ f$ is injective

  Choose $m := k,\ h := f$.

- Assume $\exists\, m \in \mathbb{N},\ h : S \to \mathbb{N}_{<m} :\ h$ is injective. Then $\exists\, n \in \mathbb{N},\ i : S \to \mathbb{N}_{\leq n} :\ i$ is injective:

  1.4.1.25 $\Rightarrow \mathbb{N}_{<m} \subseteq \mathbb{N}_{\leq m}$

  Choose $n := m,\ i := h\big|_S^{\mathbb{N}_{\leq m}}$.

- Assume $\exists\, n \in \mathbb{N},\ i : S \to \mathbb{N}_{\leq n} :\ i$ is injective. Then $\exists\, x \in \mathbb{N} :\ |S| \leq x$:

  $i \in S \to \mathbb{N}_{\leq n}$

  $\Rightarrow\ i \in S \to \mathbb{N}_{<\mathsf{s}(n)}$

  Choose $x := \mathsf{s}(n)$. $|S| \leq x$:

  $\exists\, t : S \to \mathbb{N}_{<x} :\ t$ is injective:

  Choose $t := i$.

- Assume $\exists\, x \in \mathbb{N}\colon\ |S| \leq x$. Then $\exists\, k \in \mathbb{N},\ f : S \leftrightarrow \mathbb{N}_{<k}$:

  $\overset{\text{def}}{\Rightarrow}\ \exists\, u : S \to \mathbb{N}_{<x}\colon\ u$ is injective

  Let $T := u(S)$.

  Let $o := \operatorname{bcard}(T, x)$.

  Let $v : \begin{matrix} \mathbb{N}_{<o} \to T \\ z \mapsto \operatorname{elem}(T, z) \end{matrix}$.

  Choose $k := o,\ f := v^{-1} \circ \left(u\Big|_S^T\right)$.

All of these alternative definitions reference at least the sets of functions and natural numbers, which are defined later (definitions 1.2.1 and 1.4.1.1). The notion of finiteness is introduced in advance so that the definitions are ordered by category rather than by their dependencies.

Note that some proofs are still missing or not completely spelled out.

Proposition 1.1.5. Let S be a set such that S is finite, $T \subseteq S$. Then:

T is finite

Proof. $\exists\, m \in \mathbb{N},\ f : T \to \mathbb{N}_{<m}\colon\ f$ is injective:

S is finite

$\overset{\text{def}}{\Rightarrow}\ \exists\, n \in \mathbb{N},\ g : S \to \mathbb{N}_{<n}\colon\ g$ is injective

Choose $m := n,\ f := g\Big|_T$. f is injective:

1.2.18 $\Rightarrow g\Big|_T$ is injective □

Definition 1.1.6. Let U be a set, $S, T \subseteq U$. We define:

$$S \cap T\ :=\ \{x \in U\colon\ x \in S \text{ and } x \in T\}$$

Proposition 1.1.7. Let U be a set, $R, S, T \subseteq U$. Then:

$$(R \cap S) \cap T = R \cap (S \cap T)$$

Proposition 1.1.8. Let U be a set, $S, T \subseteq U$. Then:

$$S \cap T = T \cap S$$

Proposition 1.1.9. Let U be a set, $S, T \subseteq U$. Then:

$$S \cap T \subseteq S$$

Definition 1.1.10. Let U be a set, $S, T \subseteq U$. We define:

$$S \cup T\ :=\ \{x \in U\colon\ x \in S \text{ or } x \in T\}$$

Proposition 1.1.11. Let U be a set, $R, S, T \subseteq U$. Then:

$$(R \cup S) \cup T = R \cup (S \cup T)$$

Proposition 1.1.12. Let U be a set, $S, T \subseteq U$. Then:

$$S \cup T = T \cup S$$

Proposition 1.1.13. Let U be a set, $S, T \subseteq U$. Then:

$$S \subseteq S \cup T$$

Definition 1.1.14. Let S be a set, $T \subseteq S$. We define:

$$S \setminus T \;:=\; \{x \in S \colon x \notin T\}$$

Definition 1.1.15. Let S, T be sets. We define:

$$S \uplus T \;:=:\; \left\{ \begin{matrix} \mathsf{l}_{S,T}(s) \\ \mathsf{r}_{S,T}(t) \end{matrix} \;\middle|\; \begin{matrix} s \in S \\ t \in T \end{matrix} \right\}$$

$$\begin{matrix} \forall\, s \in S,\, s' \in S: & \mathsf{l}_{S,T}(s) \;=\; \mathsf{l}_{S,T}(s') & \Leftrightarrow & s = s' \\ \forall\, t \in T,\, t' \in T: & \mathsf{r}_{S,T}(t) \;=\; \mathsf{r}_{S,T}(t') & \Leftrightarrow & t = t' \end{matrix}$$

Definition 1.1.16. Let S, T be sets. We define:

$$S \times T \;:=:\; \left\{ (s,t) \;\middle|\; s \in S,\, t \in T \right\}$$

$$\forall\, s \in S,\, t \in T,\, s' \in S,\, t' \in T: \quad (s,t) \;=\; (s',t') \quad \Leftrightarrow \quad s = s' \text{ and } t = t'$$

Definition 1.1.17. Let S be a set. We define:

$$\mathcal{P}(S) \;:=:\; \left\{ (T) \;\middle|\; T \subseteq S \right\}$$

$$\forall\, T \subseteq S,\, T' \subseteq S: \quad (T) \;=\; (T') \quad \Leftrightarrow \quad T = T'$$

Definition 1.1.18. Let U, I be sets; let $S_i \subseteq U$ for each $i \in I$. We define:

$$\bigcap_{i \in I} S_i \;:=\; \{x \in U \colon \forall\, j \in I \colon\, x \in S_j\}$$

Definition 1.1.19. Let U be a set, $S \subseteq \mathcal{P}(U)$. We define:

$$\bigcap S \;:=\; \bigcap_{i \in \{(T) \in S} T$$

Definition 1.1.20. Let U, I be sets; let $S_i \subseteq U$ for each $i \in I$. We define:

$$\bigcup_{i \in I} S_i \;:=\; \{x \in U \colon \exists\, j \in I \colon\, x \in S_j\}$$

Definition 1.1.21. Let U be a set, $S \subseteq \mathcal{P}(U)$. We define:

$$\bigcup S \;:=\; \bigcup_{i \in \{(T) \in S} T$$

1.2 Functions

Definition 1.2.1. Let X, Y be sets. We define:

$$X \to Y \;:=:\; \left\{ \begin{pmatrix} X \to Y \\ x \mapsto y_x \end{pmatrix} \;\middle|\; y_x \in Y \text{ for each } x \in X \right\}$$

$$\forall\, y_x \in Y\ (x \in X),\, y'_{x'} \in Y\ (x' \in X): \quad \begin{pmatrix} X \to Y \\ x \mapsto y_x \end{pmatrix} = \begin{pmatrix} X \to Y \\ x' \mapsto y'_{x'} \end{pmatrix} \quad \Leftrightarrow \quad \forall\, z \in X \colon\, y_z = y'_z$$

- We write "let $f : X \to Y$" instead of "let $f \in X \to Y$."

- We write "let $f : \begin{matrix} X \to Y \\ x \mapsto y_x \end{matrix}$" instead of "let $f := \begin{pmatrix} X \to Y \\ x \mapsto y_x \end{pmatrix}$."

Usually, functions are defined as specific subsets of Cartesian products, but the concept of bound variables enables this more convenient definition.

Definition 1.2.2. Let X, Y be sets, $f =: \begin{pmatrix} X \to Y \\ z \mapsto y_z \end{pmatrix} : X \to Y$, $x \in X$. We define:

$$f(x) := y_x$$

Definition 1.2.3. Let X, Y, Z be sets, $* : X \times Y \to Z$, $x \in X$, $y \in Y$. We define:

$$x * y := *(x, y)$$

Definition 1.2.4. Let Y be a set; let $a_n \in Y$ for each $n \in \mathbb{N}$. We define:

$$(a_n)_{n\in\mathbb{N}} : \begin{matrix} \mathbb{N} \to Y \\ m \mapsto a_m \end{matrix}$$

Definition 1.2.5. Let Y be a set, $a : \mathbb{N} \to Y$, $n \in \mathbb{N}$. We define:

$$a_n := a(n)$$

Definition 1.2.6. Let X, Y be sets, $f : X \to Y$, $S \subseteq X$. We define:

$$f(S) := \{f(x) \colon x \in S\}$$

Definition 1.2.7. Let X, Y be sets, $f : X \to Y$, $S \subseteq Y$. We define:

$$f^{-1}(S) := \{x \in X \colon f(x) \in S\}$$

Definition 1.2.8. Let X be a set. We define:

$$\mathrm{id}_X : \begin{matrix} X \to X \\ x \mapsto x \end{matrix}$$

Definition 1.2.9. Let X be a set, $A \subseteq X$, B be a set, $Y \subseteq B$, $f : X \to Y$. We define:

$$f\big|_A^B : \begin{matrix} A \to B \\ x \mapsto f(x) \end{matrix}$$

Definition 1.2.10. Let X be a set, $A \subseteq X$, Y be a set, $B \subseteq Y$, $f : X \to Y$ such that $f(A) \subseteq B$. We define:

$$f\big|_A^B : \begin{matrix} A \to B \\ x \mapsto f(x) \end{matrix}$$

Definition 1.2.11. Let X be a set, $A \subseteq X$, Y be a set, $f : X \to Y$. We define:

$$f\big|_A := f\big|_A^Y$$

Definition 1.2.12. Let X, Y, Z be sets, $f : X \to Y$, $g : Y \to Z$. We define:

$$g \circ f : \begin{matrix} X \to Z \\ x \mapsto g(f(x)) \end{matrix}$$

Definition 1.2.13. Let V, W, X, Y be sets, $f : V \to W$, $g : X \to Y$. We define:

$$f \times g : \begin{matrix} V \times X \to W \times Y \\ (v, x) \mapsto (f(v), g(x)) \end{matrix}$$

Definition 1.2.14. Let X, Y be sets, $f : X \to Y$. We define:

$$\begin{aligned} f \text{ is injective } &:\Leftrightarrow \forall\, a, b \in X,\ f(a) = f(b) \colon\ a = b \\ &\Leftrightarrow \forall\, c \in Y,\ d, e \in f^{-1}(\{c\}) \colon\ d = e \\ &\Leftrightarrow \forall\, y \in f(X) \colon\ \exists!\, x \in X \colon\ f(x) = y \\ &\Leftrightarrow X \text{ is empty or } \exists\, g : Y \to X \colon\ g \circ f = \mathrm{id}_X \end{aligned}$$

Definition 1.2.15. Let X, Y be sets, $f : X \to Y$. We define:

$$\begin{aligned} f \text{ is surjective } &:\Leftrightarrow \forall\, y \in Y \colon\ \exists\, x \in X \colon\ f(x) = y \\ &\Leftrightarrow Y \subseteq f(X) \\ &\Leftrightarrow f(X) = Y \end{aligned}$$

Definition 1.2.16. Let X, Y be sets, $f : X \to Y$. We define:

$$\begin{aligned} f \text{ is bijective } &:\Leftrightarrow f \text{ is injective and } f \text{ is surjective} \\ &\Leftrightarrow \forall\, y \in Y \colon\ \exists!\, x \in X \colon\ f(x) = y \\ &\Leftrightarrow \exists\, g : Y \to X \colon\ \big[g \circ f = \mathrm{id}_X \text{ and } f \circ g = \mathrm{id}_Y\big] \\ &\Leftrightarrow \exists!\, h : Y \to X \colon\ \big[h \circ f = \mathrm{id}_X \text{ and } f \circ h = \mathrm{id}_Y\big] \end{aligned}$$

Proposition 1.2.17. Let X be a set, $A \subseteq X$, B be a set, $Y \subseteq B$, $f : X \to Y$ such that f is injective. Then:

$f\big|_A^B$ is injective

Corollary 1.2.18. Let X be a set, $A \subseteq X$, Y be a set, $f : X \to Y$ such that f is injective. Then:

$f\big|_A$ is injective

Proposition 1.2.19. Let X be a set, $A \subseteq X$, B be a set, $Y \subseteq B$, $f : X \to Y$ such that $f\big|_A^B$ is surjective. Then:

f is surjective

Corollary 1.2.20. Let X be a set, $A \subseteq X$, Y be a set, $f : X \to Y$ such that $f\big|_A$ is surjective. Then:

f is surjective

Proposition 1.2.21. Let X be a set, $A \subseteq X$, Y be a set, $f : X \to Y$. Then:

$f\big|_A^{f(A)}$ is surjective

Definition 1.2.22. Let X, Y be sets. We define:

$$X \leftrightarrow Y \ := \ \{f : X \to Y \colon\ f \text{ is bijective}\}$$

- We write "let $f : X \leftrightarrow Y$" instead of "let $f \in X \leftrightarrow Y$."

Definition 1.2.23. Let X, Y be sets, $f : X \leftrightarrow Y$. For $g : Y \leftrightarrow X$, we define:

$$\begin{aligned} f^{-1} = g \ &:\Leftrightarrow \ g \circ f = \mathrm{id}_X \\ &\Leftrightarrow \ f \circ g = \mathrm{id}_Y \end{aligned}$$

Proposition 1.2.24. Let X, Y be sets, $f : X \leftrightarrow Y$. Then:

$\big(f^{-1}\big)^{-1} = f$

Proposition 1.2.25. Let X, Y be sets, $f : X \leftrightarrow Y$, $x \in X$. Then:

$f^{-1}(f(x)) = x$

Corollary 1.2.26. Let X, Y be sets, $f : X \leftrightarrow Y$, $y \in Y$. Then:

$f\big(f^{-1}(y)\big) = y$

1.3 Relations

Definition 1.3.1. Let S be a set. We define:

$$\mathcal{Rel}(S) \;:=:\; \left\{ (R) \;\middle|\; R \subseteq S \times S \right\}$$

$$\forall\, R \subseteq (S\times S)\,,\, R' \subseteq (S\times S): \quad (R) \;=\; (R') \quad\Leftrightarrow\quad R = R'$$

- We write "let $\prec$ be a relation on S" instead of "let $\prec \in \mathcal{Rel}(S)$."

Definition 1.3.2. Let S be a set, $\prec =: (R)$ be a relation on S, $s, t \in S$. We define:

$$s \prec t \;:\Leftrightarrow\; (s,t) \in R$$

1.4 Numbers

1.4.1 Natural numbers

Definition 1.4.1.1. $$\mathbb{N} \;:=:\; \left\{ \begin{matrix} 0 \\ \mathsf{s}(n) \end{matrix} \;\middle|\; n \in \mathbb{N} \right\}$$

$$\forall\, n \in \mathbb{N},\, n' \in \mathbb{N}: \quad \mathsf{s}(n) \;=\; \mathsf{s}(n') \quad\Leftrightarrow\quad n = n'$$

Definition 1.4.1.2.

$$1 \;:=\; \mathsf{s}(0)$$

Definition 1.4.1.3.

$$2 \;:=\; \mathsf{s}(1)$$

Definition 1.4.1.4. Let $m, n \in \mathbb{N}$. We define:

$$m + n \;:=\; \begin{cases} m & \text{if } n = 0 \\ \mathsf{s}(m+x) & \text{if } n = \mathsf{s}(x) \quad (x \in \mathbb{N}) \end{cases}$$

Proposition 1.4.1.5. Let $n \in \mathbb{N}$. Then:

$$\mathsf{s}(n) = n + 1$$

Proposition 1.4.1.6. Let $a, b, c \in \mathbb{N}$. Then:

$$(a+b)+c = a+(b+c)$$

Proof. $\left(\begin{cases} a+b & \text{if } c = 0 \\ \mathsf{s}((a+b)+x) & \text{if } c = \mathsf{s}(x) \quad (x \in \mathbb{N}) \end{cases} \right) = a + (b+c)$:

- $a + b = a + b$.
- Let $x \in \mathbb{N}$. Then $\mathsf{s}((a+b)+x) = \mathsf{s}(a+(b+x))$:

  1.4.1.6 $\Rightarrow (a+b)+x = a+(b+x)$

  $\Rightarrow\;\; \mathsf{s}((a+b)+x) = \mathsf{s}(a+(b+x))$

□

Lemma 1.4.1.7. Let $n \in \mathbb{N}$. Then:

$$0 + n = n$$

Proof. $\left(\begin{cases} 0 & \text{if } n = 0 \\ \mathsf{s}(0+x) & \text{if } n = \mathsf{s}(x) \quad (x \in \mathbb{N}) \end{cases}\right) = n$:

- $0 = 0$.
- Let $x \in \mathbb{N}$. Then $\mathsf{s}(0+x) = \mathsf{s}(x)$:

  1.4.1.7 $\Rightarrow 0 + x = x$

  $\Rightarrow \quad \mathsf{s}(0+x) = \mathsf{s}(x)$

□

Lemma 1.4.1.8. Let $m, n \in \mathbb{N}$. Then:

$$\mathsf{s}(m) + n = \mathsf{s}(m+n)$$

Proof. $\left(\begin{cases} \mathsf{s}(m) & \text{if } n = 0 \\ \mathsf{s}(\mathsf{s}(m)+x) & \text{if } n = \mathsf{s}(x) \quad (x \in \mathbb{N}) \end{cases}\right) = \mathsf{s}(m+n)$:

- $\mathsf{s}(m) = \mathsf{s}(m)$.
- Let $x \in \mathbb{N}$. Then $\mathsf{s}(\mathsf{s}(m)+x) = \mathsf{s}(\mathsf{s}(m+x))$:

  1.4.1.8 $\Rightarrow \mathsf{s}(m) + x = \mathsf{s}(m+x)$

  $\Rightarrow \quad \mathsf{s}(\mathsf{s}(m)+x) = \mathsf{s}(\mathsf{s}(m+x))$

□

Proposition 1.4.1.9. Let $a, b \in \mathbb{N}$. Then:

$$a + b = b + a$$

Proof. $\left(\begin{cases} a & \text{if } b = 0 \\ \mathsf{s}(a+x) & \text{if } b = x+1 \quad (x \in \mathbb{N}) \end{cases}\right) = b + a$:

- $a = 0 + a$:

  1.4.1.7 $\Rightarrow 0 + a = a$

- Let $x \in \mathbb{N}$. Then $\mathsf{s}(a+x) = \mathsf{s}(x) + a$:

  1.4.1.8 $\Rightarrow \mathsf{s}(x) + a = \mathsf{s}(x+a)$

  $\underset{a+x = x+a}{\overset{1.4.1.9}{\Rightarrow}} \quad \mathsf{s}(x) + a = \mathsf{s}(a+x)$

□

Definition 1.4.1.10. Let $m, n \in \mathbb{N}$. We define:

$$m \leq n \;:\Leftrightarrow\; \exists\, x \in \mathbb{N}\colon\; m + x = n$$

Definition 1.4.1.11. Let $m, n \in \mathbb{N}$. We define:

$$\begin{aligned} m < n \;&:\Leftrightarrow\; m \not\geq n \\ &\Leftrightarrow\; m + 1 \leq n \\ &\Leftrightarrow\; m \leq n \text{ and } m \neq n \\ &\Leftrightarrow\; \exists\, x \in \mathbb{N}_{>}\colon\; m + x = n \end{aligned}$$

Proposition 1.4.1.12. Let $a \in \mathbb{N}$. Then:

$$a \leq a$$

Proposition 1.4.1.13. Let $a, b \in \mathbb{N}$ such that $a \leq b$ and $b \leq a$. Then:

$$a = b$$

Proposition 1.4.1.14. Let $a, b, c \in \mathbb{N}$ such that $a \leq b$ and $b \leq c$. Then:

$$a \leq c$$

Proposition 1.4.1.15. Let $a, b, c \in \mathbb{N}$ such that $a < b$ and $b \leq c$. Then:

$$a < c$$

Proposition 1.4.1.16. Let $a, b, c \in \mathbb{N}$ such that $a \leq b$ and $b < c$. Then:

$$a < c$$

Proposition 1.4.1.17. Let $n \in \mathbb{N}$. Then:

$$n \geq 0$$

Proposition 1.4.1.18. Let $n \in \mathbb{N}$ such that $n \leq 0$. Then:

$$n = 0$$

Proposition 1.4.1.19. Let $n \in \mathbb{N}$. Then:

$$n + 1 > n$$

Definition 1.4.1.20. Let $n \in \mathbb{N}$. We define:

$$\mathbb{N}_{<n} := \{m \in \mathbb{N} : m < n\}$$

Definition 1.4.1.21. Let $n \in \mathbb{N}$. We define:

$$\begin{aligned} \mathbb{N}_{\leq n} &:= \{m \in \mathbb{N} : m \leq n\} \\ &= \mathbb{N}_{<(n+1)} \end{aligned}$$

Definition 1.4.1.22. Let $n \in \mathbb{N}$. We define:

$$\begin{aligned} \mathbb{N}_{\geq n} &:= \{m \in \mathbb{N} : m \geq n\} \\ &= \mathbb{N} \setminus \mathbb{N}_{<n} \end{aligned}$$

Definition 1.4.1.23. Let $n \in \mathbb{N}$. We define:

$$\begin{aligned} \mathbb{N}_{>n} &:= \{m \in \mathbb{N} : m > n\} \\ &= \mathbb{N} \setminus \mathbb{N}_{\leq n} \\ &= \mathbb{N}_{\geq (n+1)} \end{aligned}$$

Definition 1.4.1.24.

$$\begin{aligned} \mathbb{N}_{>} &:= \mathbb{N}_{>0} \\ &= \{m \in \mathbb{N} : m > 0\} \\ &= \{n \in \mathbb{N} : n \neq 0\} \\ &= \mathbb{N} \setminus \{0\} \\ &= \{a \in \mathbb{N} : \exists b \in \mathbb{N} : b + 1 = a\} \\ &= \{c \in \mathbb{N} : \exists! d \in \mathbb{N} : d + 1 = c\} \end{aligned}$$

Proposition 1.4.1.25. Let $n \in \mathbb{N}$. Then:

$\mathbb{N}_{<n} \subseteq \mathbb{N}_{\leq n}$

Proposition 1.4.1.26. Let $n \in \mathbb{N}$. Then:

$\mathbb{N}_{<n}$ is finite

Lemma 1.4.1.27. Let $M \subseteq \mathbb{N}$, $k \in \mathbb{N}$, $f : \mathbb{N}_{\leq k} \leftrightarrow M$. Then:

$\exists\, m \in M \colon \forall\, n \in M \colon n \leq m$

Proof.

$$\begin{cases} \big[\exists\, a \in M \colon \forall\, b \in M \colon b \leq a\big] & \text{if } k = 0 \\ \big[\exists\, c \in M \colon \forall\, d \in M \colon d \leq c\big] & \text{if } k = x + 1 \quad (x \in \mathbb{N}) \end{cases} :$$

- Assume $k = 0$. Then $\exists\, a \in M \colon \forall\, b \in M \colon b \leq a$:

  Choose $a := f(0)$.

- Let $x \in \mathbb{N}$ such that $k = \mathsf{s}(x)$. Then $\exists\, c \in M \colon \forall\, d \in M \colon d \leq c$:

  Let $S := \mathbb{N}_{\leq x}$.

  1.4.1.27 $\Rightarrow \exists\, i \in M \colon \forall\, j \in f(S) \colon j \leq i$

  Choose $c := \begin{cases} f(k) & \text{if } f(k) > i \\ i & \text{if } f(k) \not> i \end{cases}$. □

Proposition 1.4.1.28. Let $M \subseteq \mathbb{N}$. Then the following are equivalent:

1. M is finite
2. M is empty or $\exists\, m \in M \colon \forall\, n \in M \colon n \leq m$
3. $\exists\, a \in \mathbb{N} \colon M \subseteq \mathbb{N}_{\leq a}$
4. $\exists\, b \in \mathbb{N} \colon M \subseteq \mathbb{N}_{<b}$

Proof.

$1 \Rightarrow 2$: Assume M is finite.

$\overset{\text{def}}{\Rightarrow}\ \exists\, l \in \mathbb{N},\, f : \mathbb{N}_{<l} \leftrightarrow M$

$$\begin{cases} M \text{ is empty} & \text{if } l = 0 \\ \big[\exists\, i \in M \colon \forall\, j \in M \colon j \leq i\big] & \text{if } l = k + 1 \quad (k \in \mathbb{N}) \end{cases} :$$

- Assume $l = 0$. Then M is empty:

  $\nexists\, c \in M$:

  Assume $\exists\, c \in M$.

  $f \in \mathbb{N}_{<l} \leftrightarrow M$

  $\overset{\text{def}}{\Rightarrow}$ f is bijective

  $\overset{\text{def}}{\Rightarrow}$ f is surjective

  $\overset{\text{def}}{\Rightarrow}\ \forall\, t \in M \colon \exists\, s \in \mathbb{N}_{<0} \colon f(s) = t$

$\underset{t:=c}{\Rightarrow}\ \exists\, s\in\mathbb{N}_{<0}\colon\ f(s)=c$

$s\in\mathbb{N}_{<0}$

$\overset{\text{def}}{\Rightarrow}\ \ s<0$

1.4.1.17 $\Rightarrow s\geq 0$

- Let $k\in\mathbb{N}$ such that $l=\mathsf{s}(k)$. Then $\exists\, i\in M\colon\ \forall\, j\in M\colon\ j\leq i$:

  1.4.1.27 $\Rightarrow \exists\, y\in M\colon\ \forall\, z\in M\colon\ z\leq y$

$2\Rightarrow 3$: Assume M is empty or $\exists\, m\in M\colon\ \forall\, n\in M\colon\ n\leq m$. Then $\exists\, a\in\mathbb{N}\colon\ M\subseteq\mathbb{N}_{\leq a}$:

- Assume M is empty.

  $\overset{\text{def}}{\Rightarrow}\ \ M=\varnothing$

  Choose $a:=0$. $M\subseteq\mathbb{N}_{\leq 0}$:

  1.1.2 $\Rightarrow \varnothing\subseteq\mathbb{N}_{\leq 0}$

  $\underset{M=\varnothing}{\Rightarrow}\ \ M\subseteq\mathbb{N}_{\leq 0}$

- Assume $\exists\, m\in M\colon\ \forall\, n\in M\colon\ n\leq m$.

  Choose $a:=m$. $M\subseteq\mathbb{N}_{\leq m}$:

  Let $x\in M$. Then $x\in\mathbb{N}_{\leq m}$:

  $x\leq m$:

  $\forall\, n\in M\colon\ n\leq m$

  $\underset{n:=x}{\Rightarrow}\ x\leq m$

$3\Rightarrow 4$: Assume $\exists\, a\in\mathbb{N}\colon\ M\subseteq\mathbb{N}_{\leq a}$. Then $\exists\, b\in\mathbb{N}\colon\ M\subseteq\mathbb{N}_{<b}$:

$M\subseteq\mathbb{N}_{\leq a}$

$\Rightarrow\ \ M\subseteq\mathbb{N}_{<\mathsf{s}(a)}$

Choose $b:=\mathsf{s}(a)$.

$4\Rightarrow 1$: Assume $\exists\, b\in\mathbb{N}\colon\ M\subseteq\mathbb{N}_{<b}$.

1.4.1.26 $\Rightarrow \mathbb{N}_{<b}$ is finite

1.1.5 $\Rightarrow M$ is finite □

Proposition 1.4.1.29. Let $a,b,c\in\mathbb{N}$ such that $a+c=b+c$. Then:

$a=b$

Proposition 1.4.1.30. Let $a,b\in\mathbb{N}$, $c\in\mathbb{N}_{>}$ such that $a\cdot c=b\cdot c$. Then:

$a=b$

Definition 1.4.1.31. Let $n\in\mathbb{N}$, $m\in\mathbb{N}_{\leq n}$. For $x\in\mathbb{N}_{\leq n}$, we define:

$n-m=x\ :\Leftrightarrow\ x+m=n$

Definition 1.4.1.32. Let $m,n\in\mathbb{N}$. We define:

$$m\cdot n\ :=\ \begin{cases}0 & \text{if } n=0\\ (m\cdot x)+m & \text{if } n=x+1\quad (x\in\mathbb{N})\end{cases}$$

Proposition 1.4.1.33. Let $n \in \mathbb{N}$. Then:

$$n \cdot 1 = n$$

Proposition 1.4.1.34. Let $a, b, c \in \mathbb{N}$. Then:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Proposition 1.4.1.35. Let $a, b \in \mathbb{N}$. Then:

$$a \cdot b = b \cdot a$$

Definition 1.4.1.36. Let $m \in \mathbb{N}_>$, $n \in \mathbb{N}$. We define:

$$m \mid n \ :\Leftrightarrow\ \exists\, x \in \mathbb{N} \colon\ m \cdot x = n$$

Definition 1.4.1.37. Let $n \in \mathbb{N}$. We define:

$$\mathrm{Div}_{\mathbb{N}}(n) \ :=\ \{m \in \mathbb{N}_> \colon\ m \mid n\}$$

Proposition 1.4.1.38. Let $m \in \mathbb{N}_>$, $n \in \mathbb{N}$ such that $m \mid n$. Then:

$$m \leq n$$

Proposition 1.4.1.39. Let $a \in \mathbb{N}_>$, $b \in \mathbb{N}$ such that $a \mid b$, $c \in \mathbb{N}$. Then the following are equivalent:

1. $a \mid c$
2. $a \mid (b + c)$

Definition 1.4.1.40. Let $n \in \mathbb{N}$. We define:

$$\begin{aligned} n \text{ is even } &:\Leftrightarrow \begin{cases} \text{true} & \text{if } n = 0 \\ x \text{ is odd} & \text{if } n = x + 1 \quad (x \in \mathbb{N}) \end{cases} \\ &\Leftrightarrow\ 2 \mid n \end{aligned}$$

- Negation: n is odd

Definition 1.4.1.41. Let $n \in \mathbb{N}$, $m \in \mathrm{Div}_{\mathbb{N}}(n)$. For $x \in \mathbb{N}$, we define:

$$\frac{n}{m} = x \ :\Leftrightarrow\ m \cdot x = n$$

Definition 1.4.1.42. Let $m, n \in \mathbb{N}$. We define:

$$m^n \ :=\ \begin{cases} 1 & \text{if } n = 0 \\ m^x \cdot m & \text{if } n = x + 1 \quad (x \in \mathbb{N}) \end{cases}$$

Definition 1.4.1.43. Let $M \subseteq \mathbb{N}$. We define:

$$M \text{ is inductive } :\Leftrightarrow\ 0 \in M \text{ and } \forall\, m \in M \colon\ m + 1 \in M$$

Lemma 1.4.1.44. Let $M \subseteq \mathbb{N}$ such that M is inductive, $n \in \mathbb{N}$. Then:

$$n \in M$$

Proof.

$$\begin{cases} n \in M & \text{if } n = 0 \\ n \in M & \text{if } n = x + 1 \quad (x \in \mathbb{N}) \end{cases} :$$

- $0 \in M$:

  M is inductive

  $\overset{\text{def}}{\Rightarrow}\ 0 \in M$

- Let $x \in \mathbb{N}$. Then $x+1 \in M$:

  1.4.1.44 $\Rightarrow x \in M$

  M is inductive

  $\overset{\text{def}}{\Rightarrow}\ \forall\, m \in M\colon\ m+1 \in M$

  $\underset{m\,:=\,x}{\Rightarrow}\ x+1 \in M$ □

Proposition 1.4.1.45 (Induction principle). Let $M \subseteq \mathbb{N}$ such that M is inductive. Then:

$$M = \mathbb{N}$$

Proof.

$\supseteq$: $\mathbb{N} \subseteq M$: Let $n \in \mathbb{N}$. Then $n \in M$:

1.4.1.44 $\Rightarrow n \in M$ □

Proposition 1.4.1.46 (Well-ordering principle). Let $M \subseteq \mathbb{N}$ such that M is nonempty. Then:

$$\exists\, m \in M\colon\ \forall\, n \in M\colon\ m \leq n$$

Proof.

Let $S := \{s \in \mathbb{N}\colon\ \forall\, t \in M\colon\ s < t\}$.

S is not inductive:

Assume S is inductive.

M is nonempty

$\overset{\text{def}}{\Rightarrow}\ \exists\, y \in M$

1.4.1.44 $\Rightarrow y \in S$

$\overset{\text{def}}{\Rightarrow}\ \forall\, z \in M\colon\ y < z$

$\underset{z\,:=\,y}{\Rightarrow}\ y < y$

$\overset{\text{def}}{\Rightarrow}\ y \neq y$

$\overset{\text{def}}{\Rightarrow}\ 0 \notin S$ or $\exists\, x \in S\colon\ x+1 \notin S$

- Assume $0 \notin S$.

  $\overset{\text{def}}{\Rightarrow}\ \exists\, u \in M\colon\ 0 \geq u$

  $\overset{\text{def}}{\Rightarrow}\ u \leq 0$

  $u \in M$

  $\underset{u\,=\,0}{\overset{1.4.1.18}{\Rightarrow}}\ 0 \in M$

  Choose $m := 0$. $\forall\, n \in M\colon\ 0 \leq n$:

  Let $n \in M$. Then $0 \leq n$:

1.4.1.17 $\Rightarrow 0 \leq n$

- Assume $\exists\, x \in S\colon\ x+1 \notin S$.

  $\overset{\text{def}}{\Rightarrow}\ \exists\, v \in M\colon\ x+1 \geq v$

  $x \in S$

  $\overset{\text{def}}{\Rightarrow}\ \forall\, w \in M\colon\ x < w$

  $\underset{w:=v}{\Rightarrow}\ x < v$

  $\overset{\text{def}}{\Rightarrow}\ x+1 \leq v$

  $v \in M$

  $\underset{v\,=\,x+1}{\overset{1.4.1.13}{\Rightarrow}}\ x+1 \in M$

  Choose $m := x+1$. $\forall\, n \in M\colon\ x+1 \leq n$:

  Let $n \in M$. Then $x+1 \leq n$:

  $\forall\, w \in M\colon\ x < w$

  $\underset{w:=n}{\Rightarrow}\ x < n$

  $\overset{\text{def}}{\Rightarrow}\ x+1 \leq n$ □

Definition 1.4.1.47. Let $M \subseteq \mathbb{N}$ such that M is nonempty. For $m \in M$, we define:

$$\begin{aligned}\min(M) = m\ &:\Leftrightarrow\ \forall\, n \in M\colon\ m \leq n\\ &\Leftrightarrow\ \forall\, l \in M,\, l \leq m\colon\ l = m\\ &\Leftrightarrow\ \nexists\, k \in M\colon\ k < m\end{aligned}$$

- Assume $\forall\, n \in M\colon\ m \leq n$. Let $l \in M$ such that $l \leq m$. Then $l = m$:

  $\forall\, n \in M\colon\ m \leq n$

  $\underset{n:=l}{\Rightarrow}\ m \leq l$

  1.4.1.13 $\Rightarrow l = m$

- Assume $\forall\, l \in M,\, l \leq m\colon\ l = m$. Then $\nexists\, k \in M\colon\ k < m$:

  Assume $\exists\, k \in M\colon\ k < m$.

  $\overset{\text{def}}{\Rightarrow}\ k \leq m$ and $k \neq m$

  $\forall\, l \in M,\, l \leq m\colon\ l = m$

  $\underset{l:=k}{\Rightarrow}\ k = m$

- Assume $\nexists\, k \in M\colon\ k < m$. Then $\forall\, n \in M\colon\ m \leq n$:

  Assume $\exists\, n \in M\colon\ m \not\leq n$.

  $\overset{\text{def}}{\Rightarrow}\ n < m$

  $\exists\, k \in M\colon\ k < m$:

  Choose $k := n$.

Well-definedness. $\exists\, a \in M,\, \big[\forall\, b \in M\colon\ a \leq b\big]\colon\ \forall\, c \in M,\, \big[\forall\, d \in M\colon\ c \leq d\big]\colon\ c = a$:

1.4.1.46 $\Rightarrow \exists\, x \in M\colon\ \forall\, y \in M\colon\ x \leq y$

Choose $a := x$. $\forall\, c \in M,\, \big[\forall\, d \in M\colon\ c \leq d\big]\colon\ c = x$:

Let $c \in M$ such that $\forall\, d \in M\colon\ c \leq d$. Then $c = x$:

$\forall\, d \in M\colon\ c \leq d$

$\underset{d:=x}{\Rightarrow}\ c \leq x$

$\forall\, y \in M\colon\ x \leq y$

$\underset{y:=c}{\Rightarrow}\ x \leq c$

1.4.1.13 $\Rightarrow c = x$ □

Definition 1.4.1.48. Let $n \in \mathbb{N}$. We define:

$$n!\ :=\ \begin{cases} 1 & \text{if } n = 0 \\ x! \cdot n & \text{if } n = x + 1 \quad (x \in \mathbb{N}) \end{cases}$$

Definition 1.4.1.49. Let $n, k \in \mathbb{N}$. We define:

$$\binom{n}{k}\ :=\ \begin{cases} 1 & \text{if } k = 0 \\ \left(\begin{cases} 0 & \text{if } n = 0 \\ \binom{m}{x} + \binom{m}{k} & \text{if } n = m + 1 \quad (m \in \mathbb{N}) \end{cases} \right) & \text{if } k = x + 1 \quad (x \in \mathbb{N}) \end{cases}$$

$$=\ \begin{cases} \frac{n!}{k! \cdot (n-k)!} & \text{if } n \geq k \\ 0 & \text{if } n \ngeq k \end{cases}$$

1.4.1.50 Inductive Sums and Products

Definition 1.4.1.50.1. Let $n \in \mathbb{N}$; let $a_i \in \mathbb{N}$ for each $i \in \mathbb{N}_{<n}$. We define:

$$\sum_{i=0}^{n-1} a_i\ :=\ \begin{cases} 0 & \text{if } n = 0 \\ \left(\sum\limits_{j=0}^{m-1} a_j \right) + a_m & \text{if } n = m + 1 \quad (m \in \mathbb{N}) \end{cases}$$

Proposition 1.4.1.50.2. Let $n \in \mathbb{N}$; let $a_i, b_i \in \mathbb{N}$ for each $i \in \mathbb{N}_{<n}$. Then:

$$\sum_{j=0}^{n-1} (a_j + b_j) = \left(\sum_{k=0}^{n-1} a_k \right) + \left(\sum_{l=0}^{n-1} b_l \right)$$

Proposition 1.4.1.50.3. Let $n \in \mathbb{N}$; let $a_i \in \mathbb{N}$ for each $i \in \mathbb{N}_{<n}$; let $m \in \mathbb{N}_{\leq n}$. Then:

$$\sum_{j=0}^{m-1} a_j \leq \sum_{k=0}^{n-1} a_k$$

Proposition 1.4.1.50.4. Let $n \in \mathbb{N}$; let $a_i \in \mathbb{N}$ for each $i \in \mathbb{N}_{<n}$; let $j \in \mathbb{N}_{<n}$. Then:

$$a_j \leq \sum_{k=0}^{n-1} a_k$$

Proposition 1.4.1.50.5. Let $n, a \in \mathbb{N}$. Then:

$$\sum_{i=0}^{n-1} a = n \cdot a$$

Proposition 1.4.1.50.6. Let $n \in \mathbb{N}$. Then:

$$\sum_{i=0}^{n-1} i = \binom{n}{2}$$

Definition 1.4.1.50.7. Let $n \in \mathbb{N}$; let $a_i \in \mathbb{N}$ for each $i \in \mathbb{N}_{<n}$. We define:

$$\prod_{i=0}^{n-1} a_i := \begin{cases} 1 & \text{if } n = 0 \\ \left(\prod_{j=0}^{m-1} a_j\right) \cdot a_m & \text{if } n = m+1 \quad (m \in \mathbb{N}) \end{cases}$$

Proposition 1.4.1.50.8. Let $n \in \mathbb{N}$; let $a_i, b_i \in \mathbb{N}$ for each $i \in \mathbb{N}_{<n}$. Then:

$$\prod_{j=0}^{n-1} (a_j \cdot b_j) = \left(\prod_{k=0}^{n-1} a_k\right) \cdot \left(\prod_{l=0}^{n-1} b_l\right)$$

Proposition 1.4.1.50.9. Let $n \in \mathbb{N}$; let $a_i \in \mathbb{N}$ for each $i \in \mathbb{N}_{<n}$; let $m \in \mathbb{N}_{\leq n}$. Then:

$$\left(\prod_{j=0}^{m-1} a_j\right) \mid \left(\prod_{k=0}^{n-1} a_k\right)$$

Proposition 1.4.1.50.10. Let $n \in \mathbb{N}$; let $a_i \in \mathbb{N}_>$ for each $i \in \mathbb{N}_{<n}$; let $m \in \mathbb{N}_{\leq n}$. Then:

$$\prod_{j=0}^{m-1} a_j \leq \prod_{k=0}^{n-1} a_k$$

Proposition 1.4.1.50.11. Let $n \in \mathbb{N}$; let $a_i \in \mathbb{N}$ for each $i \in \mathbb{N}_{<n}$; let $j \in \mathbb{N}_{<n}$. Then:

$$a_j \mid \left(\prod_{k=0}^{n-1} a_k\right)$$

Proposition 1.4.1.50.12. Let $n \in \mathbb{N}$; let $a_i \in \mathbb{N}_>$ for each $i \in \mathbb{N}_{<n}$; let $j \in \mathbb{N}_{<n}$. Then:

$$a_j \leq \prod_{k=0}^{n-1} a_k$$

1.4.1.51 Prime Numbers

Definition 1.4.1.51.1. Let $n \in \mathbb{N}_{>1}$. We define:

$$\begin{aligned} n \text{ is prime } &:\Leftrightarrow \forall\, m \in \mathbb{N}_>,\, m \mid n\colon \big[m = 1 \text{ or } m = n\big] \\ &\Leftrightarrow \forall\, l \in \mathbb{N}_{>1},\, l \mid n\colon\, l = n \\ &\Leftrightarrow \mathrm{Div}_{\mathbb{N}}(n) \subseteq \{1, n\} \\ &\Leftrightarrow \mathrm{Div}_{\mathbb{N}}(n) = \{1, n\} \\ &\Leftrightarrow |\mathrm{Div}_{\mathbb{N}}(n)| = 2 \\ &\Leftrightarrow \forall\, a, b \in \mathbb{N},\, n = a \cdot b\colon \big[\big[a = 1 \text{ and } b = n\big] \text{ or } \big[a = n \text{ and } b = 1\big]\big] \\ &\Leftrightarrow \forall\, c, d \in \mathbb{N},\, n \mid (c \cdot d)\colon \big[n \mid c \text{ or } n \mid d\big] \end{aligned}$$

- Negation: n is composite

Example 1.4.1.51.2. 2 is prime

Definition 1.4.1.51.3.

$$\mathbb{P} := \{n \in \mathbb{N}_{>1}\colon n \text{ is prime}\}$$

Proposition 1.4.1.51.4. Let $n \in \mathbb{N}_{>1}$. Then:

$$\exists\, p \in \mathbb{P}\colon\, p \mid n$$

Theorem 1.4.1.51.5 (Euclid's theorem). $\mathbb{P}$ is infinite

Proof. Assume $\mathbb{P}$ is finite.

$\overset{\text{def}}{\Rightarrow}\ \exists\, n \in \mathbb{N},\ f : \mathbb{N}_{<n} \leftrightarrow \mathbb{P}$

Let $a := \prod_{i=0}^{n-1} f(i)$.

1.4.1.50.10 $\Rightarrow 1 \leq a$

Let $b := a + 1$.

1.4.1.19 $\Rightarrow b > a$

1.4.1.16 $\Rightarrow b > 1$

1.4.1.51.4 $\Rightarrow \exists p \in \mathbb{P}\colon\ p \mid b$

$\Rightarrow\ p \mid (a+1)$

1.4.1.50.11 $\Rightarrow f\big(f^{-1}(p)\big) \mid a$

$\underset{f(f^{-1}(p)) = p}{\overset{1.2.26}{\Rightarrow}}\ p \mid a$

1.4.1.39 $\Rightarrow p \mid 1$

1.4.1.38 $\Rightarrow p \leq 1$

$p \in \mathbb{P}$

$\overset{\text{def}}{\Rightarrow}\ p > 1$ □

Proposition 1.4.1.51.6. Let $p \in \mathbb{P}$, $m \in \mathbb{N}$, $n \in \mathbb{N}_>$. Then the following are equivalent:

1. $p \mid m$
2. $p \mid m^n$
3. $p^n \mid m^n$

Definition 1.4.1.52. Let $m, n \in \mathbb{N}$. We define:

$$\begin{aligned} m \text{ and } n \text{ are coprime } &:\Leftrightarrow \forall\, a \in \mathbb{N}_>,\ a \mid m,\ a \mid n\colon\ a = 1 \\ &\Leftrightarrow \mathrm{Div}_{\mathbb{N}}(m) \cap \mathrm{Div}_{\mathbb{N}}(n) \subseteq \{1\} \\ &\Leftrightarrow \mathrm{Div}_{\mathbb{N}}(m) \cap \mathrm{Div}_{\mathbb{N}}(n) = \{1\} \\ &\Leftrightarrow \nexists\, p \in \mathbb{P}\colon\ \big[p \mid m \text{ and } p \mid n\big] \end{aligned}$$

1.4.2 Cardinal numbers

Lemma 1.4.2.1. Let $m, n \in \mathbb{N}$, $f : \mathbb{N}_{<m} \leftrightarrow \mathbb{N}_{<n}$. Then:

$m = n$

Definition 1.4.2.2. $\mathcal{C}rd\ :=:\ \big\{\, |S| \;\big|\; S \text{ is a set} \,\big\}$

$\forall$ sets S, S' : $\quad |S| \;=\; |S'| \quad\Leftrightarrow\quad \exists\, \S : S \leftrightarrow S'$

$\mathbb{N} \subseteq\colon \mathcal{C}rd$ via

$\forall\, n \in \mathbb{N}\colon \quad n \;=\colon |\mathbb{N}_{<n}|$

Well-definedness. Let $m, n \in \mathbb{N}$ such that $|\mathbb{N}_{<m}| = |\mathbb{N}_{<n}|$. Then $m = n$:

$|\mathbb{N}_{<m}| = |\mathbb{N}_{<n}|$

$\overset{\text{def}}{\Rightarrow}\ \exists\, f : \mathbb{N}_{<m} \leftrightarrow \mathbb{N}_{<n}$

1.4.2.1 $\Rightarrow m = n$ □

Definition 1.4.2.3. Let $\mathbf{x} =: |X|, \mathbf{y} =: |Y| \in \mathcal{Crd}$. We define:

$$\mathbf{x} \to \mathbf{y} \ := \ X \to Y$$

- We write "let $\varphi : \mathbf{x} \to \mathbf{y}$" instead of "let $\varphi \in \mathbf{x} \to \mathbf{y}$."

Definition 1.4.2.4. Let $\mathbf{x} =: |X| \in \mathcal{Crd}$. We define:

$$\mathrm{id}_{\mathbf{x}} \ := \ \mathrm{id}_X$$

Definition 1.4.2.5. Let $\mathbf{x} =: |X|, \mathbf{y} =: |Y| \in \mathcal{Crd}$. We define:

$$\begin{aligned} \mathbf{x} \leftrightarrow \mathbf{y} \ &:= \ \{\varphi : \mathbf{x} \to \mathbf{y} : \ \varphi \text{ is bijective}\} \\ &= \ X \leftrightarrow Y \end{aligned}$$

- We write "let $\varphi : \mathbf{x} \leftrightarrow \mathbf{y}$" instead of "let $\varphi \in \mathbf{x} \leftrightarrow \mathbf{y}$."

Definition 1.4.2.6. Let $\mathbf{x} =: |X|, \mathbf{y} =: |Y| \in \mathcal{Crd}$. We define:

$$\mathbf{x} \leq \mathbf{y} \ :\Leftrightarrow\ \exists\, f : \mathbf{x} \to \mathbf{y} : \ f \text{ is injective}$$

Definition 1.4.2.7. Let $\mathbf{x}, \mathbf{y} \in \mathcal{Crd}$. We define:

$$\mathbf{x} < \mathbf{y} \ :\Leftrightarrow\ \mathbf{x} \leq \mathbf{y} \text{ and } \mathbf{x} \neq \mathbf{y}$$

Definition 1.4.2.8. Let $\mathbf{x} =: |X|, \mathbf{y} =: |Y| \in \mathcal{Crd}$. We define:

$$\mathbf{x} + \mathbf{y} \ := \ |X \uplus Y|$$

Definition 1.4.2.9. Let $\mathbf{x} =: |X|, \mathbf{y} =: |Y| \in \mathcal{Crd}$. We define:

$$\mathbf{x} \cdot \mathbf{y} \ := \ |X \times Y|$$

Definition 1.4.2.10. Let $\mathbf{x} =: |X|, \mathbf{y} =: |Y| \in \mathcal{Crd}$. We define:

$$\mathbf{x}^{\mathbf{y}} \ := \ |Y \to X|$$

Proposition 1.4.2.11. Let S be a set. Then:

$$|\mathcal{P}(S)| = 2^{|S|}$$

Definition 1.4.2.12. Let $M \subseteq \mathbb{N}$, $n \in \mathbb{N}$ such that $n < |M|$, $m := \min(M)$. We define:

$$\mathrm{elem}(M, n) \ := \ \begin{cases} m & \text{if } n = 0 \\ \mathrm{elem}(M \setminus \{m\}, x) & \text{if } n = x + 1 \quad (x \in \mathbb{N}) \end{cases}$$

Definition 1.4.2.13. Let $M \subseteq \mathbb{N}$, $n \in \mathbb{N}$. We define:

$$\mathrm{bcard}(M, n) \ := \ \begin{cases} 0 & \text{if } n = 0 \\ \left(\begin{cases} \mathsf{s}(\mathrm{bcard}(M \setminus \{\min(M)\}, x)) & \text{if } M \text{ is nonempty} \\ 0 & \text{if } M \text{ is empty} \end{cases} \right) & \text{if } n = x + 1 \quad (x \in \mathbb{N}) \end{cases}$$

1.4.3 Integers

Definition 1.4.3.1. $\mathbb{Z} :=: \left\{ \mathsf{d}(n,m) \;\middle|\; n,m \in \mathbb{N} \right\}$

$$\forall\, n,m \in \mathbb{N},\, n',m' \in \mathbb{N}: \quad \mathsf{d}(n,m) \;=\; \mathsf{d}(n',m') \quad :\Leftrightarrow \quad n+m' = n'+m$$

Reflexivity. Let $a,b \in \mathbb{N}$. Then $a+b = a+b$. □

Symmetry. Let $a,b \in \mathbb{N}$, $c,d \in \mathbb{N}$ such that $a+d = c+b$. Then $c+b = a+d$. □

Transitivity. Let $a,b \in \mathbb{N}$, $c,d \in \mathbb{N}$, $e,f \in \mathbb{N}$ such that $a+d = c+b$ and $c+f = e+d$. Then $a+f = e+b$:

$$\begin{aligned}
&a+d = c+b \\
&\Rightarrow \quad (a+d)+f = (c+b)+f \\
&\overset{\substack{1.4.1.9 \\ c+b = b+c}}{\Rightarrow} \quad (a+d)+f = (b+c)+f \\
&\overset{\substack{1.4.1.6 \\ (b+c)+f = b+(c+f)}}{\Rightarrow} \quad (a+d)+f = b+(c+f) \\
&\overset{\substack{\Rightarrow \\ c+f = e+d}}{\Rightarrow} \quad (a+d)+f = b+(e+d) \\
&\overset{\substack{1.4.1.6 \\ (b+e)+d = b+(e+d)}}{\Rightarrow} \quad (a+d)+f = (b+e)+d \\
&\overset{\substack{1.4.1.9 \\ b+e = e+b}}{\Rightarrow} \quad (a+d)+f = (e+b)+d \\
&\overset{\substack{1.4.1.6 \\ (a+d)+f = a+(d+f)}}{\Rightarrow} \quad a+(d+f) = (e+b)+d \\
&\overset{\substack{1.4.1.9 \\ d+f = f+d}}{\Rightarrow} \quad a+(f+d) = (e+b)+d \\
&\overset{\substack{1.4.1.6 \\ (a+f)+d = a+(f+d)}}{\Rightarrow} \quad (a+f)+d = (e+b)+d \\
&1.4.1.29 \Rightarrow a+f = e+b
\end{aligned}$$

□

$$\begin{aligned}
&\mathbb{N} \;\subseteq:\; \mathbb{Z} \quad \text{via} \\
\forall\, x \in \mathbb{N}: \quad &x \;=:\; \mathsf{d}(x,0)
\end{aligned}$$

Well-definedness. Let $x,y \in \mathbb{N}$ such that $\mathsf{d}(x,0) = \mathsf{d}(y,0)$. Then $x = y$:

$$\begin{aligned}
&\mathsf{d}(x,0) = \mathsf{d}(y,0) \\
&\overset{\text{def}}{\Rightarrow} \quad x+0 = y+0 \\
&\Rightarrow \quad x = y
\end{aligned}$$

□

Definition 1.4.3.2. Let $a =: \mathsf{d}(n_a,m_a), b =: \mathsf{d}(n_b,m_b) \in \mathbb{Z}$. We define:

$$a+b \;:=\; \mathsf{d}(n_a+n_b, m_a+m_b)$$

Proposition 1.4.3.3. Let $a,b,c \in \mathbb{Z}$. Then:

$$(a+b)+c = a+(b+c)$$

Proposition 1.4.3.4. Let $a,b \in \mathbb{Z}$. Then:

$$a+b = b+a$$

Definition 1.4.3.5. Let $a =: \mathsf{d}(n_a, m_a) \in \mathbb{Z}$. We define:

$$-a \;:=\; \mathsf{d}(m_a, n_a)$$

Definition 1.4.3.6. Let $b =: \mathsf{d}(n_b, m_b), a =: \mathsf{d}(n_a, m_a) \in \mathbb{Z}$. We define:

$$\begin{aligned} b - a \;&:=\; \mathsf{d}(n_b + m_a, m_b + n_a) \\ &=\; b + (-a) \end{aligned}$$

Proposition 1.4.3.7. Let $b, a \in \mathbb{Z}$. Then:

$$\mathsf{d}(b, a) = b - a$$

Definition 1.4.3.8. Let $a =: (n_a - m_a), b =: (n_b - m_b) \in \mathbb{Z}$. We define:

$$a \leq b \;:\Leftrightarrow\; n_a + m_b \leq n_b + m_a$$

Definition 1.4.3.9. Let $a, b \in \mathbb{Z}$. We define:

$$\begin{aligned} a < b \;&:\Leftrightarrow\; a \ngeq b \\ &\Leftrightarrow\; a + 1 \leq b \\ &\Leftrightarrow\; a \leq b \text{ and } a \neq b \end{aligned}$$

Definition 1.4.3.10. Let $a \in \mathbb{Z}$. We define:

$$\mathbb{Z}_{<a} \;:=\; \{b \in \mathbb{Z} \colon\; b < a\}$$

Definition 1.4.3.11. Let $a \in \mathbb{Z}$. We define:

$$\begin{aligned} \mathbb{Z}_{\leq a} \;&:=\; \{b \in \mathbb{Z} \colon\; b \leq a\} \\ &=\; \mathbb{Z}_{<(a+1)} \end{aligned}$$

Definition 1.4.3.12. Let $a \in \mathbb{Z}$. We define:

$$\begin{aligned} \mathbb{Z}_{\geq a} \;&:=\; \{b \in \mathbb{Z} \colon\; b \geq a\} \\ &=\; \mathbb{Z} \setminus \mathbb{Z}_{<a} \end{aligned}$$

Definition 1.4.3.13. Let $a \in \mathbb{Z}$. We define:

$$\begin{aligned} \mathbb{Z}_{>a} \;&:=\; \{b \in \mathbb{Z} \colon\; b > a\} \\ &=\; \mathbb{Z} \setminus \mathbb{Z}_{\leq a} \\ &=\; \mathbb{Z}_{\geq (a+1)} \end{aligned}$$

Definition 1.4.3.14. Let $a \in \mathbb{Z}$. We define:

$$\begin{aligned} \mathbb{Z}_{\lneq a} \;&:=\; \{b \in \mathbb{Z} \colon\; b \neq a\} \\ &=\; \mathbb{Z}_{<a} \cup \mathbb{Z}_{>a} \end{aligned}$$

Definition 1.4.3.15.

$$\begin{aligned} \mathbb{Z}_{<} \;&:=\; \mathbb{Z}_{<0} \\ &=\; \{a \in \mathbb{Z} \colon\; a < 0\} \end{aligned}$$

Definition 1.4.3.16.

$$\begin{aligned} \mathbb{Z}_{\leq} \;&:=\; \mathbb{Z}_{\leq 0} \\ &=\; \{a \in \mathbb{Z} \colon\; a \leq 0\} \end{aligned}$$

Definition 1.4.3.17.

$$\begin{aligned}\mathbb{Z}_{\geq} &:= \mathbb{Z}_{\geq 0} \\ &= \{a \in \mathbb{Z} \colon a \geq 0\} \\ &= \mathbb{N}\end{aligned}$$

Definition 1.4.3.18.

$$\begin{aligned}\mathbb{Z}_{>} &:= \mathbb{Z}_{>0} \\ &= \{a \in \mathbb{Z} \colon a > 0\} \\ &= \mathbb{N}_{>}\end{aligned}$$

Definition 1.4.3.19.

$$\begin{aligned}\mathbb{Z}_{\lneq} &:= \mathbb{Z}_{\lneq 0} \\ &= \{a \in \mathbb{Z} \colon a \neq 0\} \\ &= \mathbb{Z}_{<} \cup \mathbb{Z}_{>}\end{aligned}$$

Definition 1.4.3.20. Let $a \in \mathbb{Z}$. We define:

$$|a| := \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a \ngeq 0 \end{cases}$$

Definition 1.4.3.21. Let $a =: (n_a - m_a), b =: (n_b - m_b) \in \mathbb{Z}$. We define:

$$a \cdot b := \mathtt{d}((n_a \cdot n_b) + (m_a \cdot m_b), (n_a \cdot m_b) + (m_a \cdot n_b))$$

Proposition 1.4.3.22. Let $a, b, c \in \mathbb{Z}$. Then:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Proposition 1.4.3.23. Let $a, b \in \mathbb{Z}$. Then:

$$a \cdot b = b \cdot a$$

Definition 1.4.3.24. Let $a =: (n_a - m_a) \in \mathbb{Z}_{\lneq}$, $b =: (n_b - m_b) \in \mathbb{Z}$. We define:

$$\begin{aligned}a \mid b &:\Leftrightarrow \exists\, x \in \mathbb{Z} \colon a \cdot x = b \\ &\Leftrightarrow |a| \mid |b|\end{aligned}$$

Definition 1.4.3.25. Let $b \in \mathbb{Z}$. We define:

$$\mathrm{Div}_{\mathbb{Z}}(b) := \{a \in \mathbb{Z}_{\lneq} \colon a \mid b\}$$

Definition 1.4.3.26. Let $b \in \mathbb{Z}$, $a \in \mathrm{Div}_{\mathbb{Z}}(b)$. For $x \in \mathbb{Z}$, we define:

$$\frac{b}{a} = x :\Leftrightarrow a \cdot x = b$$

Definition 1.4.3.27. Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$. We define:

$$a^n := \begin{cases} 1 & \text{if } n = 0 \\ a^x \cdot a & \text{if } n = x + 1 \quad (x \in \mathbb{N}) \end{cases}$$

Proposition 1.4.3.28. Let $a, b, c \in \mathbb{Z}$ such that $a + c = b + c$. Then:

$$a = b$$

Proposition 1.4.3.29. Let $a, b \in \mathbb{Z}$, $c \in \mathbb{Z}_{\lneq}$ such that $a \cdot c = b \cdot c$. Then:

$$a = b$$

Proposition 1.4.3.30. Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Then:

$$(a \cdot b)^n = a^n \cdot b^n$$

1.4.3.31 Prime Numbers

Proposition 1.4.3.31.1. Let $p \in \mathbb{P}$, $a \in \mathbb{Z}$, $n \in \mathbb{N}_>$. Then the following are equivalent:

1. $p \mid a$
2. $p \mid a^n$
3. $p^n \mid a^n$

Definition 1.4.3.32. Let $a, b \in \mathbb{Z}$. We define:

$$\begin{aligned} a \text{ and } b \text{ are coprime } &:\Leftrightarrow \forall\, c{\in}\mathbb{Z}_>,\, c \mid a,\, c \mid b\colon\ c = 1 \\ &\Leftrightarrow \forall\, d{\in}\mathbb{Z}_{\leqslant},\, d \mid a,\, d \mid b\colon\ |d| = 1 \\ &\Leftrightarrow \mathrm{Div}_{\mathbb{Z}}(a) \cap \mathrm{Div}_{\mathbb{Z}}(b) \subseteq \{1, -1\} \\ &\Leftrightarrow \mathrm{Div}_{\mathbb{Z}}(a) \cap \mathrm{Div}_{\mathbb{Z}}(b) = \{1, -1\} \\ &\Leftrightarrow \nexists\, p{\in}\mathbb{P}\colon\ \big[p \mid a \text{ and } p \mid b\big] \end{aligned}$$

1.4.4 Rational numbers

Definition 1.4.4.1. $\mathbb{Q} :=: \left\{ \mathsf{q}(n,m) \;\middle|\; n \in \mathbb{Z},\, m \in \mathbb{N}_> \right\}$

$$\forall\, n{\in}\mathbb{Z},\, m{\in}\mathbb{N}_>,\, n'{\in}\mathbb{Z},\, m'{\in}\mathbb{N}_>\colon\quad \mathsf{q}(n,m) \;=\; \mathsf{q}(n',m') \quad :\Leftrightarrow \quad n \cdot m' = n' \cdot m$$

$$\begin{aligned} &\mathbb{Z} \;\subseteq\colon\; \mathbb{Q} \quad \text{via} \\ \forall\, x{\in}\mathbb{Z}\colon\quad &x \;=\colon\; \mathsf{q}(x,1) \end{aligned}$$

Definition 1.4.4.2. Let $a =: \mathsf{q}(n_a, m_a), b =: \mathsf{q}(n_b, m_b) \in \mathbb{Q}$. We define:

$$a + b \;:=\; \mathsf{q}\big((n_a \cdot m_b) + (n_b \cdot m_a)\,, m_a \cdot m_b\big)$$

Definition 1.4.4.3. Let $a =: \mathsf{q}(n_a, m_a) \in \mathbb{Q}$. We define:

$$-a \;:=\; \mathsf{q}(-n_a, m_a)$$

Definition 1.4.4.4. Let $b =: \mathsf{q}(n_b, m_b), a =: \mathsf{q}(n_a, m_a) \in \mathbb{Q}$. We define:

$$\begin{aligned} b - a \;&:=\; \mathsf{q}\big((n_b \cdot m_a) - (n_a \cdot m_b)\,, m_b \cdot m_a\big) \\ &=\; b + (-a) \end{aligned}$$

Definition 1.4.4.5. Let $a =: \mathsf{q}(n_a, m_a), b =: \mathsf{q}(n_b, m_b) \in \mathbb{Q}$. We define:

$$a \leq b \;:\Leftrightarrow\; n_a \cdot m_b \leq n_b \cdot m_a$$

Definition 1.4.4.6. Let $a, b \in \mathbb{Q}$. We define:

$$\begin{aligned} a < b \;&:\Leftrightarrow\; a \not\geq b \\ &\Leftrightarrow\; a \leq b \text{ and } a \neq b \end{aligned}$$

Definition 1.4.4.7. Let $a \in \mathbb{Q}$. We define:

$$\mathbb{Q}_{<a} \;:=\; \{b{\in}\mathbb{Q}\colon\ b < a\}$$

Definition 1.4.4.8. Let $a \in \mathbb{Q}$. We define:

$$\mathbb{Q}_{\leq a} \;:=\; \{b{\in}\mathbb{Q}\colon\ b \leq a\}$$

Definition 1.4.4.9. Let $a \in \mathbb{Q}$. We define:

$$\begin{aligned}\mathbb{Q}_{\geq a} &:= \{b \in \mathbb{Q} \colon b \geq a\} \\ &= \mathbb{Q} \setminus \mathbb{Q}_{<a}\end{aligned}$$

Definition 1.4.4.10. Let $a \in \mathbb{Q}$. We define:

$$\begin{aligned}\mathbb{Q}_{>a} &:= \{b \in \mathbb{Q} \colon b > a\} \\ &= \mathbb{Q} \setminus \mathbb{Q}_{\leq a}\end{aligned}$$

Definition 1.4.4.11. Let $a \in \mathbb{Q}$. We define:

$$\begin{aligned}\mathbb{Q}_{\lneq a} &:= \{b \in \mathbb{Q} \colon b \neq a\} \\ &= \mathbb{Q}_{<a} \cup \mathbb{Q}_{>a}\end{aligned}$$

Definition 1.4.4.12.

$$\begin{aligned}\mathbb{Q}_{<} &:= \mathbb{Q}_{<0} \\ &= \{a \in \mathbb{Q} \colon a < 0\}\end{aligned}$$

Definition 1.4.4.13.

$$\begin{aligned}\mathbb{Q}_{\leq} &:= \mathbb{Q}_{\leq 0} \\ &= \{a \in \mathbb{Q} \colon a \leq 0\}\end{aligned}$$

Definition 1.4.4.14.

$$\begin{aligned}\mathbb{Q}_{\geq} &:= \mathbb{Q}_{\geq 0} \\ &= \{a \in \mathbb{Q} \colon a \geq 0\}\end{aligned}$$

Definition 1.4.4.15.

$$\begin{aligned}\mathbb{Q}_{>} &:= \mathbb{Q}_{>0} \\ &= \{a \in \mathbb{Q} \colon a > 0\}\end{aligned}$$

Definition 1.4.4.16.

$$\begin{aligned}\mathbb{Q}_{\lneq} &:= \mathbb{Q}_{\lneq 0} \\ &= \{a \in \mathbb{Q} \colon a \neq 0\} \\ &= \mathbb{Q}_{<} \cup \mathbb{Q}_{>}\end{aligned}$$

Definition 1.4.4.17. Let $a \in \mathbb{Q}$. We define:

$$|a| := \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a \ngeq 0 \end{cases}$$

Definition 1.4.4.18. Let $a =: \mathsf{q}(n_a, m_a), b =: \mathsf{q}(n_b, m_b) \in \mathbb{Q}$. We define:

$$a \cdot b := \mathsf{q}(n_a \cdot n_b, m_a \cdot m_b)$$

Definition 1.4.4.19. Let $a \in \mathbb{Q}$, $n \in \mathbb{N}$. We define:

$$a^n := \begin{cases} 1 & \text{if } n = 0 \\ a^x \cdot a & \text{if } n = x + 1 \quad (x \in \mathbb{N}) \end{cases}$$

Definition 1.4.4.20. Let $a \in \mathbb{Q}$, $b \in \mathbb{Z}$ such that $a \neq 0$ or $b \geq 0$. We define:

$$a^b := \begin{cases} a^b & \text{if } b \geq 0 \\ \frac{1}{a^{-b}} & \text{if } b \ngeq 0 \end{cases}$$

Definition 1.4.4.21. Let $b \in \mathbb{Q}$, $a \in \mathbb{Q}_{\lneq}$. For $x \in \mathbb{Q}$, we define:

$$\frac{b}{a} = x :\Leftrightarrow a \cdot x = b$$

1.4.4.22 Sequences

Definition 1.4.4.22.1.

$$\mathcal{S}_{\mathbb{Q}} \;:=\; \mathbb{N} \to \mathbb{Q}$$

- We write "let a be a rational sequence" instead of "let $a \in \mathcal{S}_{\mathbb{Q}}$."

Definition 1.4.4.22.2. Let a be a rational sequence, $l \in \mathbb{Q}$. We define:

$$a \text{ converges to } l \;:\Leftrightarrow\; \forall\, \varepsilon \in \mathbb{Q}_{>} \colon\, \exists\, n \in \mathbb{N} \colon\, \forall\, m \in \mathbb{N}_{\geq n} \colon\, |a_m - l| < \varepsilon$$

Definition 1.4.4.22.3. Let a be a rational sequence. We define:

$$a \text{ is convergent } \;:\Leftrightarrow\; \exists\, l \in \mathbb{Q} \colon\, a \text{ converges to } l$$

- Negation: a is divergent

Definition 1.4.4.22.4. Let a be a rational sequence such that a is convergent. For $l \in \mathbb{Q}$, we define:

$$\lim(a) = l \;:\Leftrightarrow\; a \text{ converges to } l$$

Definition 1.4.4.22.5. Let $a_n \in \mathbb{Q}$ for each $n \in \mathbb{N}$; let $s := (a_m)_{m \in \mathbb{N}}$; assume s is convergent. We define:

$$\lim_{n \to \infty} a_n \;:=\; \lim(s)$$

Definition 1.4.4.22.6. Let a be a rational sequence. We define:

$$a \text{ is Cauchy } \;:\Leftrightarrow\; \forall\, \varepsilon \in \mathbb{Q}_{>} \colon\, \exists\, n \in \mathbb{N} \colon\, \forall\, l, m \in \mathbb{N}_{\geq n} \colon\, |a_l - a_m| < \varepsilon$$

Definition 1.4.4.22.7. Let a, b be rational sequences. We define:

$$a + b \;:=\; (a_n + b_n)_{n \in \mathbb{N}}$$

Definition 1.4.4.22.8. Let a be a rational sequence. We define:

$$-a \;:=\; (-a_n)_{n \in \mathbb{N}}$$

Definition 1.4.4.22.9. Let b, a be rational sequences. We define:

$$\begin{aligned} b - a \;&:=\; (b_n - a_n)_{n \in \mathbb{N}} \\ &=\; b + (-a) \end{aligned}$$

Definition 1.4.4.22.10. Let a, b be rational sequences. We define:

$$a \cdot b \;:=\; (a_n \cdot b_n)_{n \in \mathbb{N}}$$

1.4.5 Real numbers

Definition 1.4.5.1. $\mathbb{R} \;:=:\; \left\{ [r] \;\middle|\; r \text{ is a rational sequence such that } r \text{ is Cauchy} \right\}$

$$\begin{aligned} \forall\, r \in \mathcal{S}_{\mathbb{Q}},\, r \text{ is Cauchy},\, r' \in \mathcal{S}_{\mathbb{Q}},\, r' \text{ is Cauchy} : \quad [r] \;=\; [r'] \quad &:\Leftrightarrow \quad r - r' \text{ converges to } 0 \\ &\Leftrightarrow \quad \forall\, \varepsilon \in \mathbb{Q}_{>} \colon\, \exists\, n \in \mathbb{N} \colon\, \forall\, m \in \mathbb{N}_{\geq n} \colon\, |r_m - {r'}_m| < \varepsilon \end{aligned}$$

$$\begin{aligned} \mathbb{Q} \;&\subseteq\colon \mathbb{R} \quad \text{via} \\ \forall\, x \in \mathbb{Q} : \quad x \;&=\colon [(x)_{k \in \mathbb{N}}] \end{aligned}$$

Definition 1.4.5.2. Let $a =: [r_a], b =: [r_b] \in \mathbb{R}$. We define:

$$a + b \;:=\; [r_a + r_b]$$

Definition 1.4.5.3. Let $a =: [r_a] \in \mathbb{R}$. We define:

$$-a \;:=\; [-r_a]$$

Definition 1.4.5.4. Let $b =: [r_b], a =: [r_a] \in \mathbb{R}$. We define:

$$\begin{aligned} b - a \;&:=\; [r_b - r_a] \\ &=\; b + (-a) \end{aligned}$$

Definition 1.4.5.5. Let $a =: [r_a], b =: [r_b] \in \mathbb{R}$. We define:

$$a \leq b \;:\Leftrightarrow\; \forall\, \varepsilon \in \mathbb{Q}_{>} \colon \exists\, n \in \mathbb{N} \colon \forall\, m \in \mathbb{N}_{\geq n} \colon\; r_{am} \leq r_{bm} + \varepsilon$$

Definition 1.4.5.6. Let $a, b \in \mathbb{R}$. We define:

$$\begin{aligned} a < b \;&:\Leftrightarrow\; a \ngeq b \\ &\Leftrightarrow\; a \leq b \text{ and } a \neq b \end{aligned}$$

Definition 1.4.5.7. Let $a \in \mathbb{R}$. We define:

$$\mathbb{R}_{<a} \;:=\; \{b \in \mathbb{R} \colon\; b < a\}$$

Definition 1.4.5.8. Let $a \in \mathbb{R}$. We define:

$$\mathbb{R}_{\leq a} \;:=\; \{b \in \mathbb{R} \colon\; b \leq a\}$$

Definition 1.4.5.9. Let $a \in \mathbb{R}$. We define:

$$\begin{aligned} \mathbb{R}_{\geq a} \;&:=\; \{b \in \mathbb{R} \colon\; b \geq a\} \\ &=\; \mathbb{R} \setminus \mathbb{R}_{<a} \end{aligned}$$

Definition 1.4.5.10. Let $a \in \mathbb{R}$. We define:

$$\begin{aligned} \mathbb{R}_{>a} \;&:=\; \{b \in \mathbb{R} \colon\; b > a\} \\ &=\; \mathbb{R} \setminus \mathbb{R}_{\leq a} \end{aligned}$$

Definition 1.4.5.11. Let $a \in \mathbb{R}$. We define:

$$\begin{aligned} \mathbb{R}_{\lneq a} \;&:=\; \{b \in \mathbb{R} \colon\; b \neq a\} \\ &=\; \mathbb{R}_{<a} \cup \mathbb{R}_{>a} \end{aligned}$$

Definition 1.4.5.12.

$$\begin{aligned} \mathbb{R}_{<} \;&:=\; \mathbb{R}_{<0} \\ &=\; \{a \in \mathbb{R} \colon\; a < 0\} \end{aligned}$$

- We write "let $a < 0$" instead of "let $a \in \mathbb{R}_{<}$."

Definition 1.4.5.13.

$$\begin{aligned} \mathbb{R}_{\leq} \;&:=\; \mathbb{R}_{\leq 0} \\ &=\; \{a \in \mathbb{R} \colon\; a \leq 0\} \end{aligned}$$

- We write "let $a \leq 0$" instead of "let $a \in \mathbb{R}_{\leq}$."

Definition 1.4.5.14.

$$\begin{aligned}\mathbb{R}_{\geq} &:= \mathbb{R}_{\geq 0} \\ &= \{a \in \mathbb{R} \colon a \geq 0\}\end{aligned}$$

- We write "let $a \geq 0$" instead of "let $a \in \mathbb{R}_{\geq}$."

Definition 1.4.5.15.

$$\begin{aligned}\mathbb{R}_{>} &:= \mathbb{R}_{>0} \\ &= \{a \in \mathbb{R} \colon a > 0\}\end{aligned}$$

- We write "let $a > 0$" instead of "let $a \in \mathbb{R}_{>}$."

Definition 1.4.5.16.

$$\begin{aligned}\mathbb{R}_{\lesseqgtr} &:= \mathbb{R}_{\lesseqgtr 0} \\ &= \{a \in \mathbb{R} \colon a \neq 0\} \\ &= \mathbb{R}_{<} \cup \mathbb{R}_{>}\end{aligned}$$

Definition 1.4.5.17. Let $a =: [r_a], b =: [r_b] \in \mathbb{R}$. We define:

$$a \cdot b := [r_a \cdot r_b]$$

Definition 1.4.5.18. Let $a \in \mathbb{R}$, $n \in \mathbb{N}$. We define:

$$a^n := \begin{cases} 1 & \text{if } n = 0 \\ a^x \cdot a & \text{if } n = x + 1 \quad (x \in \mathbb{N}) \end{cases}$$

Definition 1.4.5.19. Let $a \in \mathbb{R}$, $b \in \mathbb{Z}$ such that $a \neq 0$ or $b \geq 0$. We define:

$$a^b := \begin{cases} a^b & \text{if } b \geq 0 \\ \frac{1}{a^{-b}} & \text{if } b \ngeq 0 \end{cases}$$

Definition 1.4.5.20. Let $b \in \mathbb{R}$, $a \in \mathbb{R}_{\lesseqgtr}$. For $x \in \mathbb{R}$, we define:

$$\frac{b}{a} = x :\Leftrightarrow a \cdot x = b$$

Proposition 1.4.5.21. Let $a, b \in \mathbb{R}$, $n \in \mathbb{N}$. Then:

$$(a \cdot b)^n = a^n \cdot b^n$$

Corollary 1.4.5.22. Let $b \in \mathbb{R}$, $a \in \mathbb{R}_{\lesseqgtr}$, $n \in \mathbb{N}_{>}$. Then:

$$\left(\frac{b}{a}\right)^n = \frac{b^n}{a^n}$$

Definition 1.4.5.23. Let $a \geq 0$, $n \in \mathbb{N}$. For $r \geq 0$, we define:

$$\sqrt[n]{a} = r :\Leftrightarrow r^n = a$$

Definition 1.4.5.24. Let $a \geq 0$. We define:

$$\sqrt{a} := \sqrt[2]{a}$$

Definition 1.4.5.25. Let $a \in \mathbb{R}$. We define:

$$\begin{aligned} a \text{ is rational } &:\Leftrightarrow a \in \mathbb{Q} \\ &\Leftrightarrow \exists\, b \in \mathbb{Z}_{\neq}, c \in \mathbb{Z}\colon a = \frac{c}{b} \\ &\Leftrightarrow \exists!\, d \in \mathbb{Z}_{>}, e \in \mathbb{Z}, d \text{ and } e \text{ are coprime}\colon a = \frac{e}{d} \end{aligned}$$

Theorem 1.4.5.26. Let $p \in \mathbb{P}$, $n \in \mathbb{N}_{>1}$. Then:

$\sqrt[n]{p}$ is irrational

Proof. Assume $\sqrt[n]{p}$ is rational.

$\overset{\text{def}}{\Rightarrow}$ $\exists\, a \in \mathbb{Z}_{>}, b \in \mathbb{Z}, a$ and b are coprime: $\sqrt[n]{p} = \frac{b}{a}$

$\overset{\text{def}}{\Rightarrow}$ $\left(\frac{b}{a}\right)^n = p$

$\underset{\left(\frac{b}{a}\right)^n = \frac{b^n}{a^n}}{\overset{1.4.5.22}{\Rightarrow}}$ $\frac{b^n}{a^n} = p$

$\overset{\text{def}}{\Rightarrow}$ $a^n \cdot p = b^n$

$p \mid b^n$:

$\exists\, x \in \mathbb{Z}\colon p \cdot x = b^n$:

Choose $x := a^n$.

1.4.3.31.1 $\Rightarrow p \mid b$

$\overset{\text{def}}{\Rightarrow}$ $\exists\, y \in \mathbb{Z}\colon p \cdot y = b$

$n \in \mathbb{N}_{>1}$

$\overset{\text{def}}{\Rightarrow}$ $n > 1$

$\overset{\text{def}}{\Rightarrow}$ $\exists\, m \in \mathbb{N}_{>}\colon 1 + m = n$

$\underset{1 + m = m + 1}{\overset{1.4.1.9}{\Rightarrow}}$ $m + 1 = n$

$m \in \mathbb{N}_{>}$

$\overset{\text{def}}{\Rightarrow}$ $\exists\, l \in \mathbb{N}\colon 1 + l = m$

$\underset{1 + l = l + 1}{\overset{1.4.1.9}{\Rightarrow}}$ $l + 1 = m$

$a^n \cdot p = b^n$

$\Rightarrow$ $a^n \cdot p = b^m \cdot b$

$\Rightarrow$ $a^n \cdot p = \left(b^l \cdot b\right) \cdot b$

$\underset{p \cdot y = b}{\Rightarrow}$ $a^n \cdot p = \left(b^l \cdot (p \cdot y)\right) \cdot (p \cdot y)$

1.4.3.29 $\Rightarrow a^n = \left(b^l \cdot (p \cdot y)\right) \cdot y$

$p \mid a^n$:

$\exists\, z \in \mathbb{Z}\colon p \cdot z = a^n$:

Choose $z := \left(b^l \cdot y\right) \cdot y$.

1.4.3.31.1 $\Rightarrow p \mid a$

$\exists\, q \in \mathbb{P}\colon \big[q \mid a \text{ and } q \mid b\big]$:

Choose $q := p$.

a and b are coprime

$\overset{\text{def}}{\Rightarrow}$ $\nexists\, r \in \mathbb{P}\colon \big[r \mid a \text{ and } r \mid b\big]$ □

Example 1.4.5.27. $\sqrt{2}$ is irrational

Proof.

1.4.1.51.2 $\Rightarrow$ 2 is prime

1.4.5.26 $\Rightarrow$ $\sqrt[2]{2}$ is irrational □

Chapter 2

Algebra

2.1 Isomorphisms

This section contains definitions that can be used to determine whether a function constitutes an isomorphism between two structures, in a generic way that is independent of the details of the particular structures. If the equality condition of a kind of structure is based purely on these definitions, certain well-definedness proofs can be omitted.

Definition 2.1.1. Let X, Y be sets, $\varphi : X \leftrightarrow Y$, $x \in X$. We define:

$$\varphi[x] \;:=\; \varphi(x)$$

This definition is trivial, but its importance becomes apparent in the context of the other variants.

Lemma 2.1.2. Let X, Y be sets, $\varphi : X \leftrightarrow Y$, $x \in X$. Then:

$$\varphi^{-1}[\varphi[x]] = x$$

Definition 2.1.3. Let X, Y be sets, $\varphi : X \leftrightarrow Y$, $f : X \to X$. We define:

$$\varphi[f] \;:=\; \varphi \circ \left(f \circ \varphi^{-1}\right)$$

Lemma 2.1.4. Let X, Y be sets, $\varphi : X \leftrightarrow Y$, $f : X \to X$. Then:

$$\varphi^{-1}[\varphi[f]] = f$$

Definition 2.1.5. Let X, Y be sets, $\varphi : X \leftrightarrow Y$, $* : X \times X \to X$. We define:

$$\varphi[*] \;:=\; \varphi \circ \left(* \circ (\varphi \times \varphi)^{-1}\right)$$

Lemma 2.1.6. Let X, Y be sets, $\varphi : X \leftrightarrow Y$, $* : X \times X \to X$. Then:

$$\varphi^{-1}[\varphi[*]] = *$$

Definition 2.1.7. Let X, Y be sets, $\varphi : X \leftrightarrow Y$, $\prec$ be a relation on X. We define:

$$\varphi[\prec] \;:=\; \left(\{y =: (s,t) \in (Y \times Y) \colon \varphi^{-1}(s) \prec \varphi^{-1}(t)\}\right)$$

Lemma 2.1.8. Let X, Y be sets, $\varphi : X \leftrightarrow Y$, $\prec$ be a relation on X. Then:

$$\varphi^{-1}[\varphi[\prec]] = \prec$$

2.2 Magmas

Definition 2.2.1. $\mathcal{M}gm :=: \left\{ [S,*] \;\middle|\; S \text{ is a set, } * : S\times S \to S \right\}$

$\forall$ sets S, $*:S\times S\to S$, sets S', $*':S'\times S'\to S'$: $[S,*] = [S',*'] \;\Leftrightarrow\; \exists\,\S : S\leftrightarrow S' :\; \S[*] = *'$

- We write "let $\mathbf{M}$ be a magma" instead of "let $\mathbf{M}\in\mathcal{M}gm$."

Definition 2.2.2. Let $\mathbf{M}=:[M,*]$ be a magma. We define:

$\mathbf{M}$ is associative $:\Leftrightarrow \forall\, a,b,c\in M :\; (a*b)*c = a*(b*c)$

Definition 2.2.3. Let $\mathbf{M}=:[M,*]$ be a magma. We define:

$\mathbf{M}$ is commutative $:\Leftrightarrow \forall\, a,b\in M :\; a*b = b*a$

Definition 2.2.4. Let $\mathbf{M}=:[M,*], \mathbf{N}=:[N,\star]$ be magmas. We define:

$\mathbf{M}\to\mathbf{N} := \{f : M\to N :\; \forall\, a,b\in M :\; f(a*b) = f(a)\star f(b)\}$

- We write "let $\varphi : \mathbf{M}\to\mathbf{N}$" instead of "let $\varphi\in\mathbf{M}\to\mathbf{N}$."

Definition 2.2.5. Let $\mathbf{M}=:[M,*]$ be a magma. We define:

$\mathrm{id}_{\mathbf{M}} := \mathrm{id}_M$

Definition 2.2.6. Let $\mathbf{M}=:[M,*], \mathbf{N}=:[N,\star]$ be magmas. We define:

$$\begin{aligned}\mathbf{M}\leftrightarrow\mathbf{N} &:= \{\varphi : \mathbf{M}\to\mathbf{N} :\; \varphi \text{ is bijective}\}\\ &= \{f : M\leftrightarrow N :\; \forall\, a,b\in M :\; f(a*b) = f(a)\star f(b)\}\end{aligned}$$

- We write "let $\varphi : \mathbf{M}\leftrightarrow\mathbf{N}$" instead of "let $\varphi\in\mathbf{M}\leftrightarrow\mathbf{N}$."

Proposition 2.2.7. Let $\mathbf{M},\mathbf{N}$ be magmas. Then the following are equivalent:

1. $\exists\,\varphi : \mathbf{M}\leftrightarrow\mathbf{N}$
2. $\mathbf{M} = \mathbf{N}$

Proposition 2.2.8. Let $\mathbf{M}=:[M,*], \mathbf{N}=:[N,\star]$ be magmas, $\varphi : \mathbf{M}\leftrightarrow\mathbf{N}$. Then:

$\varphi^{-1}\in\mathbf{N}\leftrightarrow\mathbf{M}$

Definition 2.2.9. Let S be a set. We define:

$$\mathcal{BT}(S) :=: \left\{ \begin{pmatrix} (s) \\ a\hat{}b \end{pmatrix} \;\middle|\; \begin{matrix} s\in S \\ a,b\in\mathcal{BT}(S) \end{matrix} \right\}$$

$$\begin{aligned} &\forall\, s\in S, s'\in S :\quad (s) = (s') \;\Leftrightarrow\; s = s'\\ &\forall\, a,b\in\mathcal{BT}(S), a',b'\in\mathcal{BT}(S) :\quad a\hat{}b = a'\hat{}b' \;\Leftrightarrow\; a = a' \text{ and } b = b'\end{aligned}$$

$$\begin{aligned} &S \subseteq : \mathcal{BT}(S) \quad \text{via}\\ &\forall\, x\in S :\quad x =: (x)\end{aligned}$$

Definition 2.2.10. Let S be a set, $T := \mathcal{BT}(S)$. We define:

$$\mathrm{Free}_{\mathcal{M}gm}(S) := [T, \begin{pmatrix} T\times T\to T \\ (a,b)\mapsto a\hat{}b \end{pmatrix}]$$

Definition 2.2.11. Let $\mathbf{M}=:[M,*]$ be a magma, $S\subseteq M$. We define:

$$\begin{aligned}\mathbf{M} \text{ is free on } S &:\Leftrightarrow \mathbf{M} = \mathrm{Free}_{\mathcal{M}gm}(S)\\ &\Leftrightarrow \forall\,\mathbf{N}=:[N,\star]\in\mathcal{M}gm,\; f : S\to N :\; \exists!\,\varphi : \mathbf{M}\to\mathbf{N} :\; \varphi\big|_S = f\end{aligned}$$

Definition 2.2.12. Let $\mathbf{M}=:[M,*]$ be a magma. We define:

$\mathbf{M}$ is free $:\Leftrightarrow \exists\, S\subseteq M :\; \mathbf{M}$ is free on S