Math Basics

— MATH ABC —

• Why is an axiomatic approach to Math necessary?

- **Example 1**. *Russell's Paradox*: The naive point of view that "A set is any collection of elements sharing some common property" leads to logical contradictions as follows. Namely, let us say that a naive set X is *normal* if X is not an element of itself, i.e., $X \notin X$, and *abnormal* if $X \in X$. Let $\mathcal{X}$ be the collection of all the normal naive sets, that is, $\mathcal{X}$ is the naive set of elements X sharing the common property $X \notin X$. *Then the naive set $\mathcal{X}$ is not normal, and not abnormal.* (WHY) Hence the naive definition of a set leads to logical contradictions **(!)**

- **Example 2**. *Berry/Richard's Paradox*: The naive point of view about numbers leads to logical contradictions as follows: Let us think that we "know" what the natural numbers are –without defining them formally. It is clear that there are natural numbers which cannot be described by less than sixty words in English. Hence the smallest such number n_0 satisfies:
"n_0 is the least natural number which cannot be described by less that sixty words in English."
OTOH, the above phrase describes n_0 in less than sixty words, contradiction **(!)**

1. Basics: Sets, Maps, Relations, . . .

Axiomatic point of view for sets

All entities under consideration are sets, and for any sets X, A one has:

- ***Either*** $X \in A$ [read "X belongs to A" or "X is element of A"].
- ***Or*** $X \notin A$ [read "X does not belong to A" or "X is not an element of A"].

• Notation. $A := \{X \mid X \in A\}$ [read "A is the set of all (the sets, or elements) X such that $X \in A$"].

In particular, every set A is the collection of elements X having the (tautological) property $X \in A$. Finally, the collection of all sets is subject to the following system of axioms, called the Zermelo-Fraenkel System of Axioms, for short (ZF), Google it! From the system of axioms (ZF) will follow that $X \notin X$ for all sets X, and that *the collection of all sets is not a set.*

Precautionary NOTE: There several ways to present (ZF), in particular the numbering of the axioms as well as the precise content could vary. But as a whole, the resulting systems of axioms are logically equivalent to each other.

AXIOMS & (immediate) CONSEQUENCES/APPLICATIONS (Google it!)

---

1. ***Axiom of extensionality***
   i) The collection $\emptyset$ which has no elements, i.e., $X \notin \emptyset$ for all X, is a set.
   ii) If A, B are sets, then $A = B$ iff they have the same elements, i.e.,

$$A = B \ \text{ iff } \ (X \in A \Rightarrow X \in B) \ \& \ (X \in B \Rightarrow X \in A).$$

Example 1.1. $\{\emptyset, A, \#, 1, \emptyset, A, \#, \#\} = \{1, A, \emptyset, \#\} = \{\#, A, A, 1, \emptyset, 1\}$.

Definition 1.2. We say that $A \subset B$ [read "A is contained in B" or "A is a subset of B"] if one has:

$$X \in A \ \Rightarrow \ X \in B.$$

Ex 1.3. One has $\emptyset \subset A$ for all sets A (WHY).

---

2. ***Axiom of Specification***

Given any set A and a property $p(X)$ of the elements $X \in A$ of the set A, one has:

The collection $A_{p(X)} := \{X \in A \mid p(X) \text{ is true}\}$ is a set.

Caution! The property $p(X)$ refers to the elements X of A only, *NOT to all the sets* X.

Remark 1.4. $A_{p(X)} \subset A$ is a subset of A (WHY).

Ex 1.5. Let $A = \{\emptyset, \#, 1, \sqrt{2}, \#, \dagger\}$ and $p(X) \equiv (X \text{ is a negative number})$. Then $A_{p(X)} = \emptyset$.

Ex 1.6. Let $p(X) \equiv (X \notin X)$. Then the collection $\{X \mid p(X)\}$ is not a set (WHY).

---

3. ***Axiom of Pairing***

For any sets A, B, the collection $\{A, B\}$ is a set whose unique elements are A, B.

Consequences

a) For every set A, the collection $\{A\}$ is a set whose unique element is A (WHY).
b) Let A, B be arbitrary sets. Then the collection $\{\{A\}, \{A, B\}\}$ is a set whose unique elements are $X = \{A\}, Y = \{A, B\}$ (WHY).

Definition 1.7. $(A, B) := \{\{A\}, \{A, B\}\}$ and called the (ordered) pair with coordinates A, B.

Ex 1.8. Let A, B, A', B' be sets. Prove that $(A, B) = (A', B')$ iff $A = A'$ and $B = B'$.

---

4. ***Axiom of Union***

Let $\mathcal{F} = \{A \mid A \in \mathcal{F}\}$ be a set. Then the collection $\{X \mid \exists\, A \in \mathcal{F} \text{ s.t. } X \in A\}$ is a set, called the union of the sets $A \in \mathcal{F}$. Notation. $\cup_{A \in \mathcal{F}} A := \{X \mid \exists\, A \in \mathcal{F} \text{ s.t. } X \in A\}$.

Remark 1.9. Let A_1, A_2 be sets. Then $\mathcal{F} := \{A_1, A_2\}$ is a set (WHY). Further, one has:

$$\cup_{A \in \mathcal{F}} A = \{X \mid \exists\, A \in \{A_1, A_2\} \text{ s.t. } X \in A\} = \{X \mid X \in A_1 \text{ or } X \in A_2\} \text{ (WHY)}.$$

Hence $\cup_{A \in \mathcal{F}} A = A_1 \cup A_2$ is the usual notion of union of sets.

Ex 1.10. Let A, B, C and more general, $A_1, \ldots, A_n$ be finitely many sets. Then $\{A, B, C\}$, and more generally $\{A_1, \ldots, A_n\}$ are sets. Hence $A \cup B \cup C$ and $\cup_{i=1}^{n} A_i$ are sets.

Proposition 1.11. *Let $\mathcal{F} = \{A \mid A \in \mathcal{F}\}$ be a set. Then $\{X \mid \forall\ A \in \mathcal{F} \text{ one has } X \in A\}$ is a set, called the intersection of the sets $A \in \mathcal{F}$.*

Proof. First, the union $\cup_{A\in\mathcal{F}} A$ is a set by Axiom 4. For $X \in \cup_{A\in\mathcal{F}} A$, consider the following property $p(X) \equiv (\forall A \in \mathcal{F}$ one has $X \in A)$. Then by Axiom 2, one has that $\{X \in \cup_{A\in\mathcal{F}} A \mid p(X) \text{ is true}\}$ is a set. OTOH, this set is precisely the above defined intersection $\cap_{A\in\mathcal{F}} A$. □

Remark 1.12. Let A_1, A_2 be sets. Then $\mathcal{F} := \{A_1, A_2\}$ is a set (WHY). Further, one has:

$$\cap_{A\in\mathcal{F}} A := \{X \mid \forall A \in \{A_1, A_2\} \text{ one has } X \in A\} = \{X \mid X \in A_1 \ \& \ X \in A_2\} \text{ (WHY)}.$$

Hence $\cap_{A\in\mathcal{F}} A = A_1 \cap A_2$ is the usual notion of intersection of sets.

Ex 1.13. Let A, B, C and $A_1, \dots, A_n$ be sets. Then $A \cap B \cap C$ and $\cap_{i=1}^n A_i$ are sets.

Definition 1.14. Let A, B be sets. Then one has:

a) $A\backslash B := \{X \mid X \in A, X \notin B\}$ is a set (WHY), called the difference of the sets A and B.
b) In particular, the symmetric difference $A \vartriangle B := (A\backslash B) \cup (B\backslash A)$ is a set (WHY).
c) Given any subset $A' \subset A$, the complement $\complement_A A' := A\backslash A'$ is a set (WHY), subset of A.

Ex 1.15. Show that $A' \cap \left(\complement_A A'\right) = \emptyset$ and $A' \cup \left(\complement_A A'\right) = A$.

---

5. ***Axiom of Normality***
If A is a non-empty set, there is $X \in A$ such that A and X have no common elements.

Definition 1.16. For any set A, $s(A) := A \cup \{A\}$ is a set (WHY), called the successor of A.

Example 1.17. Let $A = \emptyset$. Then $s(\emptyset) = \{\emptyset\}$, $s\big(s(\emptyset)\big) = s(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ (WHY), etc.

As a consequences one has:

Proposition 1.18. *The following hold:*

1) *Every set A is normal, i.e., $A \notin A$. Hence $s(A)\backslash A = \{A\}$ has a unique element A.*
2) *If A and B are sets, then $A = B$ iff $s(A) = s(B)$.*

Proof. To 1): Consider the set $\{A\}$. By the Axiom of Normality, $\exists X \in \{A\}$ s.t. X and $\{A\}$ have no comment elements. OTOH, $X := A$ is the unique element of $\{A\}$, hence $X = A$ and $\{A\}$ have no common elements. In particular, since $A \in \{A\}$, one has that $A \notin X = A$, i.e., $A \notin A$. Finally, $s(A)\backslash A = \{A\}$ is clear (WHY).

To 2): The implication "⇒" id clear (WHY). The converse implication "⇐" is a little bit more involved: By contradiction, suppose that $A \neq B$, hence $A \notin \{B\}$, $B \notin \{A\}$ (WHY). Since $A \in s(A) = s(B) = B \cup \{B\}$ and $A \notin \{B\}$, one gets: $A \in B$ (WHY); similarly, $B \in A$ (WHY). Next consider the set $\{A, B\}$. By the Axiom of Normality, $\exists X \in \{A, B\}$ s.t. X and $\{A, B\}$ have no common elements. Since A, B are the only elements of $\{A, B\}$, we have the possibilities: (i) $X = A$; (ii) $X = B$. In case (i) one has: Since $B \in \{A, B\}$, and by hypothesis one has $B \in A$, it follows that the sets $X = A$ and $\{A, B\}$ have B as a common element. Therefore one cannot have $X = A$. OTOH, in case (ii), one has: The sets $X = B$ and $\{A, B\}$ cannot have any elements in common, thus implying that $A \notin B$ (WHY), **contradicting** $A \in B$**!** □

Remark 1.19. Let A be an arbitrary set. Then one has:

- $s(A)$ is the unique set satisfying $A \subset s(A)$, $A \in s(A)$, and $s(A)\backslash A$ has one element (WHY).
- $X_0 := A \subset X_1 := s(X_0) \subset X_2 := s(X_1) \subset X_3 := s(X_2) \subset \dots$ is a strictly increasing sequence of sets (WHY).

Proof. (first assertion): Since $s(A) = A \cup \{A\}$, it follows that $A \subset s(A)$ and $A \in s(A)$ (WHY). Since $A \notin A$ (WHY), one has $A \in s(A) \backslash A$ (WHY). Finally, since A is the unique element of $\{A\}$, one has: If $X \in s(A)$ and $X \neq A$, then $X \in A$ (WHY). Hence one has: $s(A) \backslash A$ has precisely one element and that element is A. Conversely, let B be a set such that $A \subset B$, $A \in B$, and $B \backslash A$ has one element. Since $A \notin A$, it follows that $A \in B \backslash A$, hence A is the unique element of $B \backslash A$ (WHY). Thus conclude that $B = A \cup \{A\}$, as claimed. □

Remark 1.20. By the second assertion of the Remark above, and has: Applying any **finite** number of times the successor to $A := \emptyset$ as above, one can consider $A_n := \{X_0, X_1, \ldots, X_n\}$ [which is a set (WHY)]. The set A_n satisfies: For all $X \in A$, $X \neq X_n$, one has: $s(X) \in A_n$. That is, A_n is "almost" closed with respect to taking successors of its elements; that is, all its element but X_n have a successor in A_n. On the other hand, from the previous axioms **does not follow** that there is **any set** A such that $\forall X \in A$ *one has* $s(X) \in A$.

---

6. ***Axiom of Infinity***

   There exists a set A satisfying: $\emptyset \in A$, and for all $X \in A$ one has $s(X) \in A$.

NOTE. By the previous two Remarks above, it follows that A cannot be finite (WHY).

---

7. ***Axiom of the Power set***

   For any set A, the collection of all its subsets $\mathcal{P}(A) := \{A' \mid A' \subset A\}$ is a set, called the power set (or exponent set, or the set of subsets) of A.

Remark 1.21. Let A, B be sets. TFH:

- For every $X \in A$, one has $\{X\} \subset A$, hence $\{X\} \in \mathcal{P}(A)$ (WHY).
- For every $X \in A, Y \in B$, one has $\{X, Y\} \subset A \cup B$, hence $\{X, Y\} \in \mathcal{P}(A \cup B)$ (WHY).
- Finally, $\{\{X\}, \{X, Y\}\} \in \mathcal{P}\big(\mathcal{P}(A \cup B)\big)$ (WHY).

Proposition 1.22. *Let A, B be given sets. Then $A \times B := \{(X, Y) \mid X \in A, Y \in B\}$ is a set, called the (Cartesian) product of the sets A and B.*

Proof. By the Remark above, it follows that $(X, Y) \in \mathcal{P}\big(\mathcal{P}(A \cup B)\big)$ for every $X \in A$, $Y \in B$. In particular, considering the property $p_{A,B}(X, Y) \equiv (X \in A,\ Y \in B)$ about the elements (X, Y) of $\mathcal{P}\big(\mathcal{P}(A \cup B)\big)$, one has $A \times B := \{(X, Y) \in \mathcal{P}\big(\mathcal{P}(A \cup B)\big) \mid p_{A,B}(X, Y) \text{ is true}\}$. □

---

8. ***Axiom Schema of Replacement***

   Let $R \subset A \times B$ be a subset. Then $\mathrm{pr}_B(R) := \{y \in B \mid \exists\, x \in A \text{ s.t. } (x, y) \in R\}$ is a set.

Correspondences & Functions/Maps

Definition/Remark 1.23. Let A, B be sets.

1) A subset $R \subset A \times B$ is called a correspondence from A to B, or between A and B.

   For a correspondence $R \subset A \times B$, one has: $pr_A(R) \subset A$, $\mathrm{pr}_B(R) \subset B$ are subsets of A, respectively B, called the projections of R.

2) A correspondence $R \subset A \times B$ is called functional, if it has the property:

$$\forall x \in A\ \exists y \in B \text{ s.t. } (x, y) \in R, \text{ and that } y \text{ is unique.}$$

In particular, if $R \subset A \times B$ is functional, then $\text{pr}_A(R) = A$ (WHY).

Definition 1.24. Let $R \subset A \times B$, $S \subset B \times C$ be correspondences.

1) Define $R^{-1} \subset B \times A$ by the rule: $(y, x) \in R^{-1} \overset{\text{def}}{\Longleftrightarrow} (x, y) \in R$. Then R^{-1} is a subset of $B \times A$ (WHY), hence correspondence from B to A, called the inverse correspondence of R.
2) Define $T \subset A \times C$ by the rule: $(x, z) \in T \overset{\text{def}}{\Longleftrightarrow} \exists y \in B$ s.t. $(x, y) \in R$ & $(y, z) \in S$. Then T is a subset of $A \times C$ (WHY), hence a correspondence from A to C, called the composition of R and S, denoted $T = S \circ R$.

Ex 1.25. Let $R \subset A \times B$, $S \subset B \times C$, $T \subset C \times D$ be correspondences. Prove/disprove/answer:

a) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$, i.e., inverses of composition is *anti-commutative.*
b) $T \circ (S \circ R) = (T \circ S) \circ R$, i.e., composition of correspondences is *associative.*

Ex 1.26. Let $R \subset A \times B$, $S \subset B \times C$, be correspondences. Prove/disprove/answer:

a) If R and S are functional correspondences, then $T = S \circ R$ is a functional correspondence.
b) Does the converse of a) hold, i.e., is it true that $\big(T \textit{ functional} \Rightarrow R, S \textit{ functional}\big)$?

Example 1.27. Let $P := \{x \mid x \text{ inhabitant of Earth}\}$, $E := \{y \mid y \text{ is email address}\}$. Then:

a) $R := \{(x, y) \mid x \text{ has email address } y\} \subset P \times E$ is a correspondence between P and E. Is R a functional correspondence?
b) $R := \{(x, h) \mid x \in P,\ h \in \mathbb{R} \text{ is the height in meters of } x\}$ is a correspondence between P and the real numbers $\mathbb{R}$. Is R a functional correspondence?
c) $S = \{(x, y) \mid y \text{ is the mother of } x\} \subset P \times P$. Is S a functional correspondence? What are, in plain English, $S \circ R$ in both cases a), b) above?

Definition 1.28. A function, or a map from a set A to a set B is a procedure f which attaches to every $x \in A$ a **unique** $y \in B$. Notation. $f : A \to B$ [read "f defined on A with values in B"] The unique $y \in B$ attached to $x \in A$ via f is denoted $y = f(x)$ and called the value of f at x.

- The set A is called the domain of f, and the set B is called the codomain of f.
- The identity map of every set A is $\text{id}_A : A \to A$ define by $\text{id}_A(x) = x$ for all $x \in A$.

Remark 1.29. We notice the following.

1) Let $R \subset A \times B$ be a functional correspondence. Then R gives rise to a function $f_R : A \to B$ by $f_R(x) = y$, where $y \in B$ is the unique element with $(x, y) \in R$ (WHY).
2) Let $f : A \to B$ be a function. Then f gives rise to a correspondence $R_f \subset A \times B$ defined by $(x, y) \in R_f \overset{\text{def}}{\Longleftrightarrow} y = f(x)$, and R_f is functional (WHY).
3) Finally, the above procedures are inverse to each other, i.e., for f and R as above, one has:

$$f_{R_f} = f, \quad R_{f_R} = R \quad \text{(WHY)}.$$

Terminology. Given $f : A \to B$, the correspondence $R_f \subset A \times B$ is called the graph of f.

Ex 1.30. Let A, B be sets. The collection $\mathrm{Maps}(A, B) := \{f \mid f : A \to B \text{ map}\}$ is a set.

[**Hint:** By the Remark above, $\mathrm{Maps}(A, B)$ is the same as $\{R \subset A \times B \mid R \text{ functional correspondence}\}$ (WHY). OTOH, the collection of correspondences between A and B is, by definition, nothing but $\mathcal{P}(A \times B)$ (WHY), hence a set (WHY); and the fact that a correspondence $R \subset A \times B$ is a functional correspondence is an assertion $p_R(x, y)$ about the elements $(x, y) \in R$ of the set of all correspondences $\mathcal{P}(A \times B)$ (WHY), etc.]

Definition 1.31. Let $f : A \to B$ be a function.

1) f is called injective, or one-to-one, if $\forall\, x_1, x_2 \in A$ one has: $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
2) f is called surjective, or onto, if $\forall\, y \in B\ \exists\, x \in A$ such that $f(x) = y$.
3) f is called bijective, if f is both injective and surjective.

Ex 1.32. For sets A, B, the collections of maps below are subsets of $\mathrm{Maps}(A, B)$:

a) $\mathrm{Inj}(A, B) := \{f \in \mathrm{Maps}(A, B) \mid f \text{ injective}\}$
b) $\mathrm{Srj}(A, B) := \{f \in \mathrm{Maps}(A, B) \mid f \text{ surjective}\}$
c) $\mathrm{Bij}(A, B) := \{f \in \mathrm{Maps}(A, B) \mid f \text{ bijective}\}$

Ex 1.33. Let $f : A \to B$ be bijective. Then $g : B \to A$ defined by $[\, g(y) = x \overset{\text{def}}{\Longleftrightarrow} f(x) = y \,]$ is a well defined function satisfying: $g(f(x)) = x$ for all $x \in A$, and $f(g(y)) = y$ for all $y \in A$.

Definition 1.34. The map g above is called the inverse map of f, denoted $f^{-1} : B \to A$.

Exercise/Definition 1.35. Let $f : A \to B$, $g : B \to C$ be maps. Define $g \circ f : A \to C$ by the rule $(g \circ f)(x) := g(f(x))$. Then $g \circ f$ is a function (WHY), called the composition of f and g.

Prove that if $f = f_R$ and $g = f_S$ for some functional correspondences $R \subset A \times B$, $S \subset B \times C$, then $g \circ f = f_{R \circ S}$.

Ex 1.36. Let $f : A \to B$, $g : B \to C$, $h : C \to D$ be maps. Prove the following:

1) The composition of maps is associative, i.e., $(f \circ g) \circ h = f \circ (g \circ h)$.
2) $\mathrm{id}_\bullet$ is neutral element for the composition of maps, i.e., $f \circ \mathrm{id}_A = f$ and $\mathrm{id}_B \circ f = f$.
3) The following hold:
   - f and g injective $\Rightarrow g \circ f$ is injective. Does the converse hold?
   - f and g surjective $\Rightarrow g \circ f$ is surjective. Does the converse hold?
   - f and g bijective $\Rightarrow g \circ f$ is bijective, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Proposition 1.37. *Let $f : A \to B$ be a map. TFH:*

1) *For every $A' \subset A$ one has: $f(A') := \{f(x) \in B \mid x \in A'\} \subset B$ is a subset, called the image of A' under f. Further, $f_* : \mathcal{P}(A) \to \mathcal{P}(B)$, $A' \mapsto f(A')$ is a map.*
2) *For every $B' \subset B$ one has: $f^{-1}(B') := \{x \in A \mid f(x) \in B'\} \subset A$ is a subset, called the preimage of B' under f. $f^* : \mathcal{P}(B) \to \mathcal{P}(A)$, $B' \mapsto f^{-1}(B')$ is a map.*

Proof. To 1): Let $R_f \subset A \times B$ be the graph of f. Then $R_{A'} := R_f \cap (A' \times B)$ is a set (WHY), and check directly that $f(A') = \mathrm{pr}_B\left(R_{A'}\right)$ (WHY), hence a subset of B. Further, f_* is a map **Ex** .... To 2): **Ex** ... □

Ex 1.38. A function $f : A \to B$ is surjective iff $f(A) = B$ iff $f_*(A) = B$.

Ex 1.39. Let A and B be sets, and $f : A \to B$ be a map. Prove/disprove the following:

1) $f_*(A' \cup A'') = f_*(A') \cup f_*(A'')$, $f_*(A' \cap A'') = f_*(A') \cap f_*(A'')$ for all $A', A'' \in \mathcal{P}(A)$.
2) $f^*(B' \cup B'') = f^*(B') \cup f^*(B'')$, $f^*(B' \cap B'') = f^*(B') \cap f^*(B'')$ for all $B', B'' \in \mathcal{P}(B)$.
3) f_* and/or f^* are injective/surjective/bijective iff f is so.

The set of natural numbers $\mathbb{N}$

Theorem 1.40. *There exists a unique set* $\mathbb{N}$*, called the* set of natural numbers*, having the following properties:*

i) $\emptyset \in \mathbb{N}$ *and* $X \in \mathbb{N} \Rightarrow s(X) \in \mathbb{N}$

ii) *For every* $X' \in \mathbb{N}$ *one has: If* $X' \neq \emptyset$*, there exists* $X \in \mathbb{N}$ *such that* $X' = s(X)$.

iii) $\mathbb{N}$ *is minimal with the property* i) *above, i.e., if* $N \subset \mathbb{N}$ *is a subset having the property* i)*, i.e.,* $\emptyset \in N$ *and* $X \in N \Rightarrow s(X) \in N$*, then* $N = \mathbb{N}$.

Proof. **Step 1.** *Existence of* $\mathbb{N}$ *satisfying* i), ii), iii): By the Infinity Axiom, there exist sets A such that:

$$(*) \qquad \emptyset \in A \quad \& \quad \big(X \in A \Rightarrow s(X) \in A\big)$$

We prove that every set A as above contains a unique subset A_0 which satisfies the conditions i), ii), iii) from the Theorem (with $\mathbb{N}$ replaced by A_0). Indeed, given a set A as above, consider

$$\mathcal{F} := \{\, A' \in \mathcal{P}(A) \mid A' \text{ satisfies condition } (*) \,\}$$

Since the sets $A' \in \mathcal{F}$ can be described by a property $p(A')$ as elements of $\mathcal{P}(A)$ (WHY), it follows that $\mathcal{F}$ is a set (of subsets of A) (WHY). Therefor, one has that

$$A_0 := \cap_{A' \in \mathcal{F}} A' \quad \textit{is a subset of } A \quad \text{(WHY)}.$$

We first claim that A_0 satisfies condition $(*)$ (with A replaced by A_0). Indeed, since all $A' \in \mathcal{F}$ satisfy $(*)$, one has: First, $\emptyset \in A'$ for all $A' \in \mathcal{F}$, hence $\emptyset \in A_0$ (WHY). Second, if $X \in A_0$, then $X \in A'$ for all $A' \in \mathcal{F}$. Thus $s(A') \in A'$ for all $A' \in \mathcal{F}$ (WHY), hence $s(X) \in A_0$.

Next we claim that A_0 satisfies i), ii), iii) from the Theorem (with $\mathbb{N}$ replaced by A_0). Indeed, one has:

- First, since A_0 satisfies $(*)$, it follows that A_0 satisfies conditions i) (WHY).
- For ii), consider all $X \in A$ s.t. there exists some subset $A_X \subset A$ satisfying the four conditions:

  (a) $\emptyset, X \in A_X$; (b) $\emptyset \neq s(X')\ \forall X' \in A_X$; (c) If $X' \neq X$, then $s(X') \in A_X$; (d) $s(X) \notin A_X$.

Then the collection $\mathcal{A}$ of all subsets A_X is a subset of $\mathcal{P}(A)$ (WHY), and one has: $A_\emptyset = \{\emptyset\}$ (WHY), and given A_X, one has that $A_{s(X)} = A_X \cup \{s(X)\}$ (WHY). **Note:** In particular, $A_\emptyset = \{\emptyset\}, A_{s(\emptyset} = \{\emptyset, \{\emptyset\}\}, A_{s(s(\emptyset))}, \ldots$ lie in $\mathcal{A}$. Finally, let $A^0 := \cup_{A_X \in \mathcal{A}} A_X$ be the union of all the sets $A_X \in \mathcal{A}$.

Claim. The set A^0 lies in $\mathcal{F}$.

Proof of Claim. **Ex** ...

In particular, by the definition of A_0, it follows that $A_0 \subset A^0$ (WHY), hence finally A_0 satisfies (ii) (WHY).

- For condition iii), we notice that if $N \subset A_0$ is a subset having property i), then N satisfies condition $(*)$ (WHY). Hence $N \in \mathcal{F}$, and therefore $A_0 \subset N$ (WHY). Thus finally $A_0 = N$, as claimed.

Step 2. *Uniqueness of* $\mathbb{N}$: Let A, B be sets satisfying condition $(*)$, and let $A_0 \subset A$, $B_0 \subset B$ be the corresponding unique subsets constructed as above. We claim that $A_0 = B_0$. Indeed, let $C := A \cup B$. Then C is a set satisfying condition $(*)$ (WHY), and $A_0, B_0 \subset C$ satisfy condition $(*)$ as well (WHY); Hence if $C_0 \subset C$ be the unique subset constructed as above for C, one has $C_0 \subset A_0, B_0$ (WHY). Hence by property iii) of the sets A_0, B_0, one has $A_0 = C_0 = B_0$ (WHY). Hence $\mathbb{N} := A_0$ is the unique set satisfying condition i), ii), iii). $\square$

Notation. Denote/identify: $\emptyset \leftrightarrow 0$, $s(\emptyset) \leftrightarrow 1$, $s\big(s(\emptyset)\big) \leftrightarrow 2$, ... thus $\mathbb{N} = \{0, 1, 2, \ldots\}$.

Remark 1.41. First, the conditions i), ii), iii) in Theorem above are equivalent to the so called Peano Axioms, or Dedeking–Peano Axioms (Google it!) Second, the last condition iii) in Theorem above is called the Induction Principle. An interpretation of the Induction Principle is the following important and extremely useful fact:

Theorem 1.42. (Induction Principle) *Let a sequence of assertions $\mathcal{P}_n$, $n \in \mathbb{N}$ be given. To prove that all $\mathcal{P}_n$, $n \in \mathbb{N}$ are true, it is sufficient to do the following:*

- Step 1. Verification step: *Prove that $\mathcal{P}_0$ is true.*
- Step 2. Induction step: *Prove that $\mathcal{P}_n \Rightarrow \mathcal{P}_{s(n)}$ for all n.*

Proof. Let $N \subset \mathbb{N}$ be the set of all $n \in \mathbb{N}$ such that $\mathcal{P}_n$ is true. Then one has: First, $0 \in N$ (WHY). Second, if $n \in N$, then $s(n) \in N$ (WHY). Hence by the property iii) of the natural numbers, one has $N = \mathbb{N}$. □

Theorem 1.43. (Weak Induction Principle) *Let a sequence of assertions $\mathcal{Q}_n$, $n \in \mathbb{N}$ be given. To prove that all the $\mathcal{Q}_n$, $n \in \mathbb{N}$ are true, it is sufficient to do the following:*

- Step 1. Verification step: *Prove that $\mathcal{Q}_0$ is true.*
- Step 2. Induction step: *Prove that $(\mathcal{Q}_0 \,\&\ldots\&\, \mathcal{Q}_n) \Rightarrow \mathcal{Q}_{s(n)}$ for all n.*

Proof. Let $\mathcal{P}_n \equiv (\mathcal{Q}_0 \,\&\ldots\&\, \mathcal{Q}_n)$. We notice that the assertions below are equivalent:

i) $\mathcal{P}_n \Rightarrow \mathcal{P}_{s(n)}$ for all $n \in \mathbb{N}$

ii) $(\mathcal{Q}_0 \,\&\ldots\&\, \mathcal{Q}_n) \Rightarrow \mathcal{Q}_{s(n)}$ for all $n \in \mathbb{N}$.

Indeed: First suppose that i) is true, or equivalently one has:

$$(\mathcal{Q}_0 \,\&\ldots\&\, \mathcal{Q}_n) \equiv \mathcal{P}_n \;\Rightarrow\; \mathcal{P}_{s(n)} \equiv (\mathcal{Q}_0 \,\&\ldots\&\, \mathcal{Q}_n \,\&\, \mathcal{Q}_{s(n)}), \quad \forall\, n \in \mathbb{N}.$$

The LHS is true iff $\mathcal{Q}_k$ is true for $0 \leqslant k \leqslant n$ (WHY), whereas the RHS is true iff $\mathcal{Q}_k$ is true for $0 \leqslant k \leqslant s(n)$ (WHY). Hence the displayed implication is true iff $(\mathcal{Q}_0 \,\&\ldots\&\, \mathcal{Q}_n) \Rightarrow \mathcal{Q}_{s(n)}$ (WHY). Second, suppose that ii) is true. Then by the discussion above, one has that $(\mathcal{Q}_0 \,\&\ldots\&\, \mathcal{Q}_n) \Rightarrow (\mathcal{Q}_0 \,\&\ldots\&\, \mathcal{Q}_n \,\&\, \mathcal{Q}_{s(n)})$ is true (WHY), hence concluding that $\mathcal{P}_n \Rightarrow \mathcal{P}_{s(n)}$ is true.

To conclude the proof, we apply the Induction Principle to the sequence of assertions $\mathcal{P}_n$, $n \in \mathbb{N}$, as follows: First, $\mathcal{P}_0 \equiv \mathcal{Q}_0$. Second, by the claim above, $\mathcal{P}_n \Rightarrow \mathcal{P}_{s(n)}$ iff $(\mathcal{Q}_0 \,\&\ldots\&\, \mathcal{Q}_n) \Rightarrow \mathcal{Q}_{s(n)}$, etc. □

- The most important application of the (Weak) Induction Principle are proofs by induction.

Cardinality of sets

One has the following famous fact, called the **Cantor-Bernstein-Schroeder Theorem** (we do not give a proof, but Google it!):

Theorem 1.44. *Let A, B be sets such that there exist injective maps $f : A \to B$ and $g : B \to A$. Then there exist bijective maps $\phi : A \to B$ as well.*

Definition 1.45. Let A, B be sets.

a) We say that $|A| \leqslant |B|$ [read "cardinality of A is less or equal to the cardinality of B"], if there exists an injective map $f : A \to B$.

b) We say that $|A| < |B|$ [read "cardinality of A is less than the cardinality of B"], if $|A| \leqslant |B|$ and there are no injective maps $f : B \to A$.

Definition 1.46. For $n \in \mathbb{N}$, the typical set with n elements $[n] \subset \mathbb{N}$ is defined as follows:
1) $[0] = \emptyset$ is the empty set.
2) If $n \neq 0$, then $[n] \subset \mathbb{N}$ is the unique subset satisfying the conditions:
   (i) $0 \notin [n]$, $1 \in [n]$, $s(n) \notin [n]$; (ii) $(\, m \neq n \;\&\; m \in [n]\,) \Rightarrow s(m) \in [n]$.

Definition 1.47. Let A be an arbitrary set.
1) A is finite and has n elements, if there is a bijection $\phi : [n] \to A$.
2) A is called infinite, if there are injective maps $\phi : [n] \to A$ for all $n \in \mathbb{N}$.

Remark 1.48. Intuitively, the set $[n]$ is the set of the first n natural numbers $\neq 0$. In particular, one has: $[1] = \{1\}$, $[2] = \{1, 2\}$, $[3] = \{1, 2, 3\}$, $[4] = \{1, 2, 3, 4\}$, etc.

Concerning typical finite sets, the hollowing holds:

Proposition 1.49. *A map $f : [n] \to [n]$ is injective if and only if f is bijective.*

Proof. We make induction on n: The case $n = 1$ is clear, because $[1] = \{1\}$ and every map $f : \{1\} \to \{1\}$ is bijective (WHY). We prove the induction step: Suppose that every injective map $f : [n] \to [n]$ is bijective. We then prove that every injective map $g : [s(n)] \to [s(n)]$ is bijective. Indeed, let $m := g(n)$, and define $h : [s(n)] \to [s(n)]$ by $h(m) = s(n)$, $h(s(n)) = m$ and $h(i) = i$ for $i \neq m, s(n)$. Then h is bijective (WHY). Hence $g_0 := h \circ g : [s(n)] \to [s(n)]$ is injective (WHY). OTOH, $g_0(s(n)) = h(g(s(n))) = h(m) = s(n)$ (WHY).

Hence since g_0 is injective, if follows that $g_0(i) \neq s(n)$ for all $i \neq s(n)$, i.e., all $i \in [n]$. Hence we conclude that $f_0 : [n] \to [n]$ by $f_0(i) = g_0(i)$ is an injective map. Hence by the induction hypothesis, f_0 is bijective. Thus $g_0 : [s(n)] \to [s(n)]$ is bijective as well (WHY). Finally, since $g_0 = h \circ g$, and h is bijective, hence so is its inverse map h^{-1} and $\mathrm{id} = h^{-1} \circ h$, we get:

$$g = \mathrm{id} \circ g = (h^{-1} \circ h) \circ g = h^{-1} \circ (h \circ g) = h^{-1} \circ g_0,$$

and therefore, g is bijective as being the composition of the bijective maps g_0 and h^{-1}. □

Theorem 1.50 (Characaterization of infinite sets). *Let A be a given set. Then A is infinite iff there exists an injective map $f : \mathbb{N} \to A$, i.e., $|\mathbb{N}| \leqslant |A|$.*

Proof. The implication "$\Leftarrow$" is proved as follows: Let $\phi : \mathbb{N} \to A$ be an injective map. For every $n \in \mathbb{N}$, consider the map $\phi_n : [n] \to A$ by $\phi_n(m) := \phi(m)$ for all $m \in [n]$. NOTE: Actually $\phi_n := \phi|_{[n]}$ is the restriction of ϕ to $[n]$. Then $\phi_n : [n] \to A$ is injective for every $n \in \mathbb{N}$ (WHY).

The implication "$\Rightarrow$" is little bit more tricky. Let $\phi_n : [n] \to A$ be given injective maps for every $n \in \mathbb{N}$, $n \neq 0$, and let $\mathcal{P}_n$ be the assertion:

$$\mathcal{P}_n \equiv \big(\exists\, \psi_n : [n] \to A \text{ injective s.t. } \psi_n(i) = \psi_m(i)\, \forall m \in [n] \;\&\; i \in [m]\big)$$

[In plain English, that means that the restriction of ψ_n to $[m] = \{1, \dots, m\}$ equals ψ_m for all $m \in \{1, \dots, n\}$.]
We prove by induction that all assertions $\mathcal{P}_n$ are true.

Step1: Verification step: $\mathcal{P}_1$ is true. Indeed, there is nothing to prove (WHY).

Step 2: Induction step: $\mathcal{P}_n \Rightarrow \mathcal{P}_{s(n)}$. We begin by proving the following:

Claim. *There exists $m \in [s(n)]$ such that $\phi_{s(n)}(m) \neq \psi_n(i)\ \forall\, i \in [n]$.*

Proof of the Claim. Indeed, *by contradiction,* suppose that the Claim does not hold. Then one must have:

$$A_{s(n)} := \phi_{s(n)}\big(\,[s(n)]\,\big) \subset \psi_n\big(\,[n]\big) =: B_n \text{ (WHY)}.$$

By definition one has: $\psi_n : [n] \to B_n$ is both injective and surjective (WHY), hence bijective. In the same way, $\phi_{s(n)} : [s(n)] \to A_{s(n)}$ is bijective as well. Hence ψ_n and $\phi_{s(n)}$ being injective, we conclude that

$$f : [s(n)] \xrightarrow{\phi_{s(n)}} A_n \subset B_n \xrightarrow{\psi_n^{-1}} [n] \subset [s(n)]$$

is an injective map (WHY). Thus by Proposition 1.42 above, it follows that f is actually bijective. On the other hand, since the canonical inclusion $[n] \subset [s(n)]$ is not surjective (WHY), it follows that f cannot be surjective, thus not bijective, contradiction! Thus the Claim holds.

Hence by the Claim there is some $m \in [s(n)]$ such that $y := \phi_{s(n)}(m) \neq \psi_n(i)\ \forall\, i \in [n]$. We conclude the proof by defining $\psi_{s(n)} : [s(n)] \to A$ as follows: $\psi_{s(n)}(i) := \psi_n(i)$ for $i \in [n]$, and $\psi_{s(n)}\big(s(n)\big) := y$. Then $\psi_{s(n)}$ is injective (WHY), and $\psi_{s(n)}(i) = \psi_n(i)$ for all $i \in [n]$.

To conclude the proof of the Proposition, recall that $B_n := \{\, \psi_n(i) \,|\, i \in [n] \,\}$, consider the set $\{B_n\}_{n\in\mathbb{N}}$ of (finite) subsets of A, and set $B := \cup_{n\in\mathbb{N}} B_n$. Then one can define $\psi : \mathbb{N} \to B \subset A$ by $\psi(n) = \psi_{s(n)}\big(s(n)\big)$; e.g., $\psi(0) = \psi_1(1)$, $\psi(1) = \psi_2(2)$, $\psi(2) = \psi_3(3)$, etc. Check that ψ is injective (WHY). □

One has the following intrinsic characterization of finite sets:

Theorem 1.51 (Characaterization of finite sets). *For a non-empty set A the following are equivalent:*

i) *A is a finite set.*
ii) *Every injective map $f : A \to A$ is bijective.*
iii) *Every surjective map $f : A \to A$ is bijective.*

Proof. We first show that the last two conditions are equivalent: iii) ⇒ ii): Let $f : A \to A$ be a surjective map. Equivalently, for every $y \in A$, there exists $x \in A$ s.t. $y = f(x)$. For every y, let $x_y \in A$ be a fixed element s.t. $f(x_y) = y$, and notice that $y_1 \neq y_2 \Rightarrow x_{y_1} \neq x_{y_2}$ (WHY). Define $g : A \to A$ by $g(y) = x_y$. Then g is a well defined function (WHY), and we claim that g is injective: Indeed, $g(y_1) = g(y_2)$ iff $x_{y_1} = x_{y_2}$ iff $y_1 = f(x_{y_1}) = f(x_{y_2}) = y_2$ (WHY). Hence by hypothesis ii), since g is injective, one has that g is bijective. Hence every $x \in A$ is of the form $x = x_y$ for a unique y satisfying $f(x) = y$. Therefore, f must be bijective as well. The proof of ii) ⇒ iii) is similar, **Ex**...

To i) ⇒ ii): Let $\phi : A \to [n]$ be a fixed bijection, and $\phi^{-1} : [n] \to A$ be its inverse map. For any map $f : A \to A$, set $g := \phi^{-1} \circ f \circ \phi : [n] \to [n]$; hence $f = \phi \circ g \circ \phi^{-1}$ as well (WHY). Since ϕ, ϕ^{-1} are bijections, one has: If f is a bijection, then g is a bijection (WHY). Conversely, if g is a bijection, then f is a bijection (WHY). Hence it is enough to show (WHY): Every injective map $g : [n] \to [n]$ is bijective. This was proved in Proposition 1.49 above.

To ii) ⇒ i): By contradiction, suppose that A is infinite. Let $\psi : \mathbb{N} \to A$ be an injective map. Define $f : A \to A$ as follows: If $x = \psi(n)$, then set $f(x) = \psi\big(s(n)\big)$, and if $x \neq \psi(n)$ for all $n \in \mathbb{N}$, then set $f(x) = x$. Then $\psi(0) \neq f(x)$ for all $x \in A$ (WHY), hence f is not surjective. Further, f is injective (WHY). Thus finally f injective but not bijective, contradiction! □

Relations

Definition/Remark 1.52. A relation on a set A is any correspondence $R \subset A \times A$. In particular, the collection of all the relations on A is nothing but the set $\mathcal{P}(A \times A)$ (WHY).

Example 1.53. On every set A one has the relations: (i) The empty relation $\emptyset \subset A \times A$. (ii) The diagonal $\Delta_A := \{(x, x) \mid x \in A\}$. (iii) The total relation $A \times A$.

Example 1.54. Let $P := \{x \mid x \text{ person living in Phila}\}$. Then $R := \{(x, y) \mid x \text{ is relative of } y\}$ is a relation on P.

Equivalence relations

Definition 1.55. Let A be a non-empty set.

1) A relation R on A, usually denoted $\sim$, which means $x \sim y \overset{\text{def}}{\longleftrightarrow} (x, y) \in R$, is called an equivalence relation on A, if it satisfies the hypotheses:

i) $\sim$ is reflexive, i.e., $x \sim x$ for all $x \in A$. Equivalently, $\Delta_A \subset R$.

ii) $\sim$ is symmetric, i.e., $x \sim y \Rightarrow y \sim x$. Equivalently, $R^{-1} = R$.

iii) $\sim$ is transitive, i.e., $(x \sim y \;\&\; y \sim z) \Rightarrow x \sim z$.

2) Give an equivalence relation $\sim$ on A, for $x \in A$, one denotes $\widehat{x} := \{x' \in A \mid x \sim x'\}$ and calls it the equivalence class of x.

Example 1.56. Let A be a non-empty set. Then one has:

a) The diagonal $\Delta_A := \{(x,x) \mid x \in A\} \subset A \times A$ is an equivalence relation, and its equivalence classes are $\widehat{x} = \{x\}$ for all $x \in A$ (WHY).

b) The total relation $A \times A$ on A is an equivalence relation on A, which has a unique equivalence class $\widehat{x} = A$ (WHY).

c) Let P be the set of people. Which relation R below on P is an equivalence relation?

(i) $xRy \overset{\text{def}}{\longleftrightarrow}$ "x is a friend of y"

(ii) $xRy \overset{\text{def}}{\longleftrightarrow}$ "x and y like the same foods"

(iii) $xRy \overset{\text{def}}{\longleftrightarrow}$ "x and y have the same friends in Patagonia."

d) A is the set of rational numbers, and define R on A by: xRy iff $x - y$ is an integer number. Is R an equivalence relation on A? If so, what are the equivalence classes?

Ex 1.57. Let $R \subset A \times A$ be a relation. Prove/disprove:

i) R is reflexive if and only if $\Delta_A \subset R$.

ii) R is symmetric if and only if $R^{-1} = R$.

iii) R is transitive if and only if $R \circ R = R$.

Definition 1.58. A partition of a set A is a set of non-empty subsets $A_i \subset A$, $i \in I$ such that $A = \cup_{i \in I} A_i$, and for all A_i, A_j one has: $A_i \cap A_j \neq \emptyset \Rightarrow A_i = A_j$.

Example 1.59. Let $A = \{0, 1, \ldots, 100\}$, $A_0, A_1, A_2 \subset A$ be the even, resp. odd, resp. the square numbers. Then $\{A_0, A_1\}$ is a partition of A, but $\{A_1, A_2\}$, $\{A_0, A_1, A_2\}$ are not (WHY).

Proposition 1.60. *Let A be a non-empty set. TFH:*

1) *The equivalence classes $\widehat{x}$ are actually subsets $\widehat{x} \subset A$, and $\{\, \widehat{x} \mid x \in X \,\}$ is a subset of $\mathcal{P}(A)$, called the set of equivalence classes of $\sim$ and usually denoted $A/\!\sim$.*

2) Characterization of Equivalence Relations:

i) *For $x, y \in A$ one has: $\widehat{x} \cap \widehat{y} \neq \emptyset$ iff $\widehat{x} = \widehat{y}$. Hence $A = \cup_{x \in A} \widehat{x}$ is a partition of A.*

ii) *Conversely, let $A = \cup_{i \in I} A_i$ be a partition of A, and define $\sim$ on A by $x \sim y$ iff $\exists\, i \in I$ s.t. $x, y \in A_i$. Then $\sim$ is an equivalence relation having $\widehat{x} = A_i$ iff $x \in A_i$.*

Proof. To 1): Let $R \subset A \times A$ be the equivalence reaction $\sim$ on A, and $\mathrm{pr}_1 : R \to A$ by $\mathrm{pr}_1(x,y) = x$ and $\mathrm{pr}_2 : R \to A$ by $\mathrm{pr}_2(x,y) = y$ be the projection on the first, respectively second coordinate. Then one has that $\mathrm{pr}_1^{-1}(x) = \{(x,x') \mid x \sim x'\}$ for every $x \in A$ (WHY), hence a subset of R (WHY). OTOH, $\widehat{x} = \mathrm{pr}_2(\{(x,x') \mid x \sim x'\})$ (WHY), and therefore, $\widehat{x} \subset A$ is a subset (WHY). Further, $A/\!\sim$ is a collection of subsets $\widehat{x}$ of the power set $\mathcal{P}(A \times A)$ such the subsets $\widehat{x}$ can be defined by an assertion $p_\sim(X)$ about the elements $X \in \mathcal{P}(A \times A)$ (WHY).[**Ex** : Write down explicitly the assertion $p_\sim(X)$ describing the equivalence classes $\widehat{x}$ as elements $\widehat{x} \in \mathcal{P}(A)$.] We thus conclude that $X/\!\sim$ is a set, subset of $\mathcal{P}(A \times A)$ (WHY).

To 2) i): Given $\widehat{x} \cap \widehat{y} \neq \emptyset$, we show that $\widehat{x} = \widehat{y}$. Indeed, if $z \in \widehat{x} \cap \widehat{y}$, then $x \sim z$ and $y \sim z$. Hence $x \sim y$ (WHY). Therefore one has: $x' \in \widehat{x}$ iff $x \sim x'$ iff $x' \sim y$ (WHY). Thus $\widehat{x} = \widehat{y}$, as claimed. Hence we conclude that $\{\, \widehat{x} \mid x \in A \,\}$ is indeed a partition of A (WHY). To 2) ii): **Ex** . . . $\square$

Order relations or **(partial) Ordering**

Definition 1.61. An order relation or a (partial) ordering on a set A is any relation on A, usually denoted $\leqslant$ [read "less or equal to"], which has the properties:

i) $\leqslant$ is reflexive, i.e., $x \leqslant x$ for all $x \in A$.

ii) $\leqslant$ is antisymmetric, i.e., $(x \leqslant y \;\&\; y \leqslant x) \Rightarrow x = y$.

iii) $\leqslant$ is transitive, i.e., $(x \leqslant y \;\&\; y \leqslant z) \Rightarrow x \leqslant z$.

Notation. If $x \leqslant y$ and $x \neq y$, we write $x < y$ [read "x strictly less than y"]. Further, in stead of $x \leqslant y$ and/or $x < y$, one also writes $y \geqslant x$ [read "y greater or equal to x"], respectively $y > x$ [read "y strictly greater than x"]. Hence one has: $x \leqslant y \overset{\text{def}}{\longleftrightarrow} y \geqslant x$, respectively $x < y \overset{\text{def}}{\longleftrightarrow} y > x$.

Ex 1.62. A reflexive relation $R \subset A \times A$ is anti-symmetric iff $R \cap R^{-1} = \Delta_A$.

Definition 1.63. Let $\leqslant$ be an ordering on A, and $B \subset A$ be a non-empty subset.

a) An element $y_B \in B$ is a minimum of B, if $\forall\, y \in B$ one has: $y \leqslant y_B \Rightarrow y = y_B$.
Notation. Let $\min(B)$ be the set of minimal elements in B, which may be empty.
Define/denote correspondingly a maximum $y^B \in B$ of B, respectively $\max(B)$.

b) An element $x_B \in A$, if it exists, is called an infimum of B, if it satisfies: First, $x_B \leqslant y$ for all $y \in B$; second, if $x \in A$ is such that $x \leqslant y$ for all $y \in B$, then $x \leqslant x_B$.
Define correspondingly a supremum $x^B \in A$ of B, provided it exists.
Notation. $\inf(B)$, respectively $\sup(B)$.

Example 1.64. Define $\leqslant$ on $\mathcal{P}(A)$ by $A' \leqslant A'' \overset{\text{def}}{\longleftrightarrow} A' \subset A''$. Then one has:

a) $\leqslant$ is a partial ordering on $\mathcal{P}(A)$ (WHY), and $\min\big(\mathcal{P}(A)\big) = \emptyset$, $\max\big(\mathcal{P}(A)\big) = A$ (WHY).
Further, if $\mathcal{F} \subset \mathcal{P}(A)$ is non-empty, then $\sup(\mathcal{F}) = \cup_{A' \in \mathcal{F}} A'$, $\inf(\mathcal{F}) = \cap_{A' \in \mathcal{F}} A'$ (WHY).

b) Let $A' := (0,1] \subset [-1,2] =: A$ endowed with the ordering of real numbers. Then $\min(A')$ does not exist (WHY), $\inf(A') = 0$ (WHY), and $\max(A') = 1 = \sup(A')$ (WHY).

Ex 1.65. In the above notations, prove/disprove/answer the following:

1) If $\min(B)$ exists, then that minimum is unique, i.e., if y'_B, y''_B are minima of B, then $y'_B = y''_B$. Correspondingly, the same for maximum.

2) If $\inf(B)$ exists, then that infimum is unique, i.e., if x', x''_B are infima of B, then $x'_B = x''_B$. Correspondingly, the same for supremum.

Ex 1.66. Prove/disprove the following:

1) If $\min(B)$ exists, then $\inf(B)$ exists, and $\inf(B) = \min(B)$. Does the converse hold? The same question, correspondingly, for $\max(B)$ and $\sup(B)$.

2) Give examples $\inf(B)$ exists, but $\min(B)$ does not.

Definition 1.67. Let $\leqslant$ be an ordering of a non-empty set A.

1) $\leqslant$ is called total ordering, if for all $x, y \in A$ one has that $x \leqslant y$ or $y \leqslant x$.

2) $\leqslant$ is called a well ordering, if $\min(A')$ exists for every non-empty subset $A' \subset A$.

Example 1.68. The following hold:

a) The set of real numbers $\mathbb{R}$ is totally ordered w.r.t the natural ordering $\leqslant$.
b) Every well ordered set A is totally ordered (WHY), but the converse does not hold (WHY).
c) Every totally ordered finite set is well ordered.

Ex 1.69. Let A be a non-empty set. Prove that the collections of all partial/total/well orderings, respectively all equivalence relations on A are sets.

Remark 1.70. Recall that given sets A, B we defined the (direct, or Cartesian) product $A\times B$. Further, given three sets A, B, C one can define $(A\times B)\times C$ and $A\times(B\times C)$ which are formally distinct sets, although there is a "canonical" bijection $(A \times B) \times C \to A \times (B \times C)$ defined by $((a, b), c) \mapsto (a, (b, c))$ (WHY). In particular, formally it is not correct to write $A \times B \times C$, because we did define triplets (a, b, c).

Ex 1.71. Try to define directly (X, Y, Z) for given sets X, Y, Z satisfying the property $(X, Y, Z) = (X', Y', Z')$ iff $X = X'$, $Y = Y'$, $Z = Z'$.

One encounters an even bigger issue when trying to define the direct (or cartesian) product of any set of sets A_i, $i \in I$.

---

9. ***Axiom of Choice***
Given $A = \{X \,|\, X \in A\} \neq \emptyset$ with $X \neq \emptyset$, for every $X \in A$ one *can choose* $x_X \in X$.

Notice that an equivalent formulation of the Axiom of Choice, for short (AC), is that one has a function $f : A \to \cup_{X\in A} X$ such that for all $X \in A$ one has $f(X) \in X$.

Ex 1.72. Prove that (AC) is equivalent to the fact that for any sets A and B, every surjective map $f : A \to B$ has a *right inverse map,* i.e., there is $g : B \to A$ such that $f \circ g = \mathrm{id}_B$.

Yet another equivalent formulation of (AC) is the existence of the direct product of any sets of sets as follows. (**Note**: for this construction one needs the definition of maps, which itself involved (HOW) the product of two sets as previously defined.) Namely, let X_i, $i \in I$ be a non-empty set of sets, $X_0 := \cup_i X_i$ be their union, and $\mathrm{Maps}(I, X_0)$ be the set of maps from I to $X_0 = \cup_i X_i$. Then the *collection of all the maps*

$$(*) \qquad f : I \to X_0 = \cup_i X_i \ \text{ satisfying } \ f(i) \in X_i \ \text{ for all } \ i \in I$$

is a *subset of* $\mathrm{Maps}(I, X_0)$ (WHY).

1) We denote the set of all the maps $f : I \to X_0$ satisfying property $(*)$ above by $\prod_{i\in I} X_i$ and call it the **(direct, or cartesian) product** of the set of sets X_i, $i \in I$.
2) The typical element in $\prod_{i\in I} X_i$ is denoted $(x_i)_i$, with the interpretation $x_i :\overset{\text{def}}{=} f(i)$. In particular, $(x_i)_i = (y_i)_i$ iff $x_i = y_i$ for all $i \in I$ (WHY).

On the other hand, from the system of first eight axioms above — the Zermelo–Fraenkel System of Axioms (ZF) — it does not follow that there is any map $f : I \to X_0$ satisfying $(*)$, hence that $\prod_i X_i$ is a non-empty set. Obviously, (AC) holds iff $\prod_i X_i \neq \emptyset$ for all $I \neq \emptyset$ and non-empty sets $X_i, i \in I$. Moreover, in the system of axioms (ZF) + (AC), one has:

$(**)$ *For every $i_0 \in I$, one has a surjective map $p_{i_0} : \prod_i X_i \to X_{i_0}$, $(x_i)_i \mapsto x_{i_0}$* (WHY).

Remark 1.73. Given sets A, B and setting $I = \{1, 2\}$ and $X_1 = A$, $X_2 = B$, the direct product $A \times B$ can be identified with $\prod_{i \in I} X_i$. Namely every $(x_1, x_2) \in X_1 \times X_2 = A \times B$ defines a unique map $f : I \to X_0 = A \cup B$ by setting $f(i) = x_i$, hence f satisfies condition $(*)$ above. Conversely, every $f : I \to X_0 = A \cup B$ satisfying condition $(*)$ above defines a unique element in $(x_1, x_2) \in A \times B$ by setting $x_1 := f(1) \in X_1 = A$, $x_2 := f(2) \in X_2 = B$.

Remark 1.74. The above Axiom of Choice is not part of the Zermelo-Fraenkel System of Axioms (ZF), which consists of the above first 8 (eight) axioms above. The (ZF) together with (AC) is denoted (ZFC). There are several equivalent formulations of (ZFC), e.g.:

Theorem 1.75. *The following systems of axioms for sets are equivalent:*

i) *(ZF) & **Axiom of Choice***
ii) *(ZF) & **Zorn's Lemma**: All partially ordered sets $A, \leqslant$ satisfy: If every non-empty totally ordered subset $A', \leqslant$ of $A, \leqslant$ has $\sup(A')$ in A, then $\max(A)$ is non-empty.*
iii) *(ZF) & **Well ordering Axiom**: Every non-empty set A admits a well ordering.*

Proof. Google it ! □

2. Arithmetic and Properties of $\mathbb{N}$

Addition and Multiplication in $\mathbb{N}$

Define on $\mathbb{N}$ the following addition and multiplication, in one word, composition laws:

- *addition* $+$ for $n \in \mathbb{N}$ by: $n + 0 :\overset{\text{def}}{=} n$, and recursively, $n + s(m) :\overset{\text{def}}{=} s(n + m)\ \forall m \in \mathbb{N}$
- *multiplication* $\cdot$ for $n \in \mathbb{N}$ by: $n \cdot 0 :\overset{\text{def}}{=} 0$, and recursively, $n \cdot s(m) :\overset{\text{def}}{=} n \cdot m + n\ \forall m \in \mathbb{N}$.

NOTE: $+$ and $\cdot$ are by no means symmetric in the arguments, therefore *rigorous proofs* are needed to show that $+$ and $\cdot$ have the necessary basic properties for computations.

Theorem 2.1. *The addition $+$ and the multiplication $\cdot$ on $\mathbb{N}$ have the following properties:*

1) *Addition $+$ satisfies:*
   - *associativity, i.e., $(k + m) + n = k + (m + n)\ \ \forall k, m, n \in \mathbb{N}$.*
   - *commutativity, i.e., $m + n = n + m\ \ \forall m, n \in \mathbb{N}$.*
   - *$0 \in \mathbb{N}$ is neutral element, i.e., $n + 0 = n = 0 + n\ \ \forall n \in \mathbb{N}$.*
2) *Multiplication $\cdot$ satisfies:*
   - *associativity, i.e., $(k \cdot m) \cdot n = k \cdot (m \cdot n)\ \ \forall k, m, n \in \mathbb{N}$.*
   - *commutativity, i.e., $m \cdot n = n \cdot m\ \ \forall m, n \in \mathbb{N}$.*
   - *$1 \in \mathbb{N}$ is neutral element, i.e., $n \cdot 1 = n = 1 \cdot n\ \ \forall n \in \mathbb{N}$.*
3) *Multiplication is distributive w.r.t. addition, i.e.,*

$$k \cdot (m + n) = k \cdot m + k \cdot n \text{ and } (m + n) \cdot k = m \cdot k + n \cdot k \qquad \forall k, m, n \in \mathbb{N}.$$

Proof. To 1): Associativity, by induction on n: Step 1. $\mathcal{P}_0$: $(k + m) + 0 = k + m = k + (m + 0)$, done! (WHY). Step 2. $\mathcal{P}_n \Rightarrow \mathcal{P}_{s(n)}$: Recall that $\mathcal{P}_{s(n)} \equiv (k + m) + s(n) = k + \big(m + s(n)\big)$. One has:

$$(k + m) + s(n) \overset{\text{why}}{=} s\big((k + m) + n)\big) \overset{\text{why}}{=} s\big(k + (m + n)\big) \overset{\text{why}}{=} k + s(m + n) \overset{\text{why}}{=} k + \big((m + s(n)\big).$$

Commutativity, by induction on n: Step 1. $\mathcal{P}_0$: $m+0=0+m$ iff $m=0+m\ \forall m$. That is proved by induction on m **Ex** ... One also has to prove that $\mathcal{P}_1$: $m+1=1+m$ is true for all $m\in\mathbb{N}$ hods **Ex** ... (HOW). Step 2. $\mathcal{P}_n\Rightarrow\mathcal{P}_{s(n)}$: Recalling that $\mathcal{P}_{s(n)}\equiv\big(m+s(n)=s(n)+m\ \forall m\in\mathbb{N}\big)$, one has:

$$m+s(n)\overset{\text{why}}{=}m+(n+1)\overset{\text{why}}{=}(m+n)+1\overset{\text{why}}{=}(n+m)+1\overset{\text{why}}{=}n+(m+1)\overset{\text{why}}{=}n+(1+m)\overset{\text{why}}{=}(n+1)+m=s(n)+m$$

To 3): Induction on k: Step 1. $\mathcal{P}_0$: $(m+n)\cdot 0=0=m\cdot 0+n\cdot 0$ (WHY). Step 2. $\mathcal{P}_k\Rightarrow\mathcal{P}_{s(k)}$: One has

$$(m+n)\cdot s(k)\overset{\text{why}}{=}(m+n)\cdot k+(m+n)\overset{\text{why}}{=}m\cdot k+n\cdot k+m+n\overset{\text{why}}{=}(m\cdot k+m)+(n\cdot k+n)=m\cdot s(k)+n\cdot s(k)$$

To 2): Make induction on n, using assertions 1), 3). □

The natural ordering $\leqslant$ *on* $\mathbb{N}$

Define on $\mathbb{N}$ the relation: $m\leqslant n\ \overset{\text{def}}{\Longleftrightarrow}\ \exists\, l\in\mathbb{N}$ s.t. $m+l=n$.

Theorem 2.2. *The relation* $\leqslant$ *on* $\mathbb{N}$ *is an ordering satisfying the following:*

1) $\leqslant$ *is* compatible *w.r.t. both addition and multiplication, i.e.,* $\forall\, k,m,n\in\mathbb{N}$ *one has:*
$$m\leqslant n\quad\Rightarrow\quad m+k\leqslant n+k,\ \ m\cdot k\leqslant n\cdot k.$$
2) *The ordering* $\leqslant$ *is a total ordering, and moreover, a well ordering of* $\mathbb{N}$.

Proof. To 1: Induction on k: Step 1. $\mathcal{P}_0$: $m\le n\Rightarrow m+0\leqslant n+0\, m\cdot k\leqslant n\cdot 0$ are obvious (WHY).
Step 2. $\mathcal{P}_k\Rightarrow\mathcal{P}_{s(k)}$: Since $m\leqslant n$, one has $m+l=n$ for some $l\in\mathbb{N}$ (WHY). Hence one has:

$$m+l=n\overset{\text{why}}{\Rightarrow}m+l+k=n+k\overset{\text{why}}{\Rightarrow}s(m+l+k)=s(n+k)\overset{\text{why}}{\Rightarrow}(m+l)+s(k)=n+s(k)\overset{\text{why}}{\Rightarrow}\big(m+s(k)\big)+l=n+s(k),$$

thus $m+s(k)\leqslant n+s(k)$. Similarly, $m+l=n\overset{\text{why}}{\Rightarrow}(m+l)\cdot k=n\cdot k$, hence $(m+l)\cdot k+(m+k)=n\cdot k+n$ (WHY). Equivalently, $(m+l)\cdot s(k)=n\cdot s(k)$ (WHY). On the other hand, setting $l':=l\cdot s(k)$, one has:

$$(m+l)\cdot s(k)=n\cdot s(k)\overset{\text{why}}{\Rightarrow}m\cdot s(k)+l\cdot s(k)=m\cdot s(k)+l'=n\cdot s(k),\quad\text{hence}\quad m\cdot s(k)\leqslant n\cdot s(k)\quad\text{(WHY)}.$$

To 2): The assertions $\mathcal{P}_n\equiv\big(\forall\, m\in\mathbb{N},\ \text{one has } m\le n \text{ or } n\le m\big)$ are true for all $n\in\mathbb{N}$. Indeed: $\mathcal{P}_0$ is true (WHY). Step 2. $\mathcal{P}_n\Rightarrow\mathcal{P}_{s(n)}$: First, if $m\le n$, then $m\leqslant s(n)$ (WHY). Hence it is left to analyze the case $n\leqslant m$, $n\neq m$. If so, $n+l'=m$ with $l'\neq 0$ (WHY), thus $l'=s(l'')$ for some $l''\in\mathbb{N}$ (WHY). Hence one has:

$$m=n+l'\overset{\text{why}}{=}n+s(l'')\overset{\text{why}}{=}s(n+l'')\overset{\text{why}}{=}s(l''+n)\overset{\text{why}}{=}l''+s(n),\quad\text{and finally,}\quad s(n)\le m\quad\text{(WHY)}.$$

Finally, $\leqslant$ is a well ordering: Indeed, let $N\subset\mathbb{N}$ be a non-empty set. Choose any $n\in N$, and do: If $n=0$, then $0=\min(\mathbb{N})$ is a minimal element of N (WHY). If $n\neq 0$, then $[n]$ is a finite totally ordered set, hence a well ordered set (WHY). Therefore, $[n]\cap N$ is non-empty (because $n\in[n]$), and has a minimal element n_0. Conclude that $n_0\in N$ satisfies $n_0=\min(N)$ (WHY). □

Proposition 2.3. *The addition* $+$*, the multiplication* $\cdot$ *and the ordering* $\leqslant$ *on* $\mathbb{N}$ *satisfy the* cancelation property*, i.e., for all* $k,m,n\in\mathbb{N}$ *the following hold:*

1) $n+k=m+k$ *iff* $n=m$*, and* $n\cdot k=m\cdot k$ *iff* $n=m$*, provided* $k\neq 0$.
2) $m+k\leqslant n+k$ *iff* $m\leqslant n$*, and* $n\cdot k\leqslant m\cdot k$ *iff* $n=m$*, provided* $k\neq 0$.

Proof. To 1): Induction on k: First, the assertion is clear for $k=0$ (WHY). Second, one has: $n+s(k)=m+s(k)$ iff $s(n+k)=s(m+k)$ (WHY) iff $n+k=m+k$ (WHY), etc. Concerning $\cdot$ one has: $n=m\Rightarrow h\cdot k=m\cdot k$ (WHY). For the converse, let $n\cdot k=m\cdot k$ be given. By contradiction, suppose that $m\neq n$, and w.l.o.g., suppose that $m<n$. Hence by definitions, there exists $l>0$ such that $m+l=n$. Therefore we have

$$m\cdot k=n\cdot k=(m+l)\cdot k=m\cdot k+l\cdot k,$$

thus we get $0=l\cdot k$ (WHY). Since $k,l\neq 0$, one has $l\cdot k\neq 0$ (WHY), contradiction! To 2): **Ex** ... □

Arithmetic in $\mathbb{N}$

Definition 2.4. Let $m, n, p \in \mathbb{N}$ be natural numbers $\mathbb{N}$.

1) Divisibility. We say that m divides n, or that m is a divisor of n, if $n = m \cdot k$ for some $k \in \mathbb{N}$. Notation. $m|n$.
2) The lowest common multiple $\operatorname{lcm}(m, n)$ of m, n is the smallest natural number having m, n as divisors. The greatest common divisor $\gcd(m, n)$ is the largest number dividing m, n. One says that m, n are coprime, if $\gcd(m, n) = 1$.
3) Prime numbers. A natural number $p \in \mathbb{N}$ is called prime number, if $p > 1$ and the only divisors of p are 1 and p.

Proposition 2.5. *In the set of natural numbers $\mathbb{N}$, the following hold:*

1) *The divisibility relation $m|n$ is a partial ordering on $\mathbb{N}$, and 1 is the only minimal element. Further the prime numbers are the minimal elements in the set $\mathbb{N}_{>1} := \{\, n \,|\, n \neq 0, 1 \,\}$.*
2) *Divisibility is compatible with addition, precisely, if $l + m = n$ and k divides two of the numbers l, m, n, then k divides all numbers l, m, n.*
3) *Every natural number $n > 1$ is a product of prime numbers.*

Proof. To 1), 2): **Ex**... (just use the definitions!) To 3): Make induction on n, and use the Induction Principle Thm in the form: *All* $\{\mathcal{P}_n\}_{n\in\mathbb{N}}$ *are true, provided* (i) $\mathcal{P}_0$ *is true* & (ii) $\big(\mathcal{P}_0, \dots, \mathcal{P}_n\big) \Rightarrow \mathcal{P}_{s(n)}$. $\square$

Theorem 2.6. *The following hold:*

1) *Division with remainder. For every $m, n \in \mathbb{N}$, $m \neq 0$, there exist* **unique** *$q, r \in \mathbb{N}$ such that $n = m \cdot q + r$, $0 \leqslant r < m$.* **Terminology.** *The numbers $q, r \in \mathbb{N}$ are called the result, respectively the remainder of the division of n by m with remainder.*
2) *Euclidean Algorithm. Suppose that $m \neq 0$, and set $r_0 := n$, $r_1 := m$, and inductively, let $r_{i-1} = q_i \cdot r_i + r_{i+1}$ be the division of r_{i-1} by r_i with remainder r_{i+1}. Then $r_{i+1} = 0$ for sufficiently large i. And if $r_i \neq 0$ and $r_{i+1} = 0$, then $r_i = \gcd(n, m)$.*
3) *Uniqueness of prime number factorization. For every $n \in \mathbb{N}$, $n \neq 0, 1$, there exist unique s and unique prime numbers $p_1 \leqslant \dots \leqslant p_s$ such that $n = p_1 \dots p_s$.*

Proof. To 1): **Ex** (make induction on m ...) To 2): Wet set $d := \gcd(m, n)$, and claim that $d|r_{k+1}$ for all $k \in \mathbb{N}$. Indeed, by induction on k, one has: Since $d|m$, $d|n$, one has (by definitions) that $d|r_0$, $d|r_1$. Hence by Proposition above, $d|r_2$. Induction step: If $d|r_{k-1}$, $d|r_k$, by loc.cit. one has: $d|r_{k+1}$ (WHY). In particular, if $i \in \mathbb{N}$ is such that $r_i \neq 0$ and $r_{i+1} = 0$, then $d|r_i$. Conversely, suppose that $r_i \neq 0$ and $r_{i+1} = 0$ for some $i \in \mathbb{N}$. We claim that $r_i|d$. Indeed, let $\mathcal{P}_k$ be the assertion: $\mathcal{P}_k \equiv r_i|r_{i-k}$, $k = 0, \dots, i$. **Ex** (prove by induction on k, that the assertion $\mathcal{P}_k$, $k = 0, \dots, i$, are true. Namely, $\mathcal{P}_0 \equiv (\, r_i|r_i \,)$ is clear. For $\mathcal{P}_1$, note that $r_{i-1} = q_i r_i + r_{i+1} = q_i r_i$; hence $r_i|r_{i-1}$ (WHY), ...) Hence finally one has that $d|r_i$ and $r_i|d$, thus $d = r_i$ (WHY), as claimed. To 3): The key point in the proof is the following:

Key Lemma. *A number $p \in \mathbb{N}$ is a prime number iff $p > 1$ and for all $m, n \in \mathbb{N}$ one has:*

$$p \,|\, (m \cdot n) \;\Rightarrow\; (\, p \,|\, m \text{ or } p \,|\, n\,)$$

Proof. (of the Key Lemma) The implication "$\Leftarrow$": We have to show that the only divisors of p are $1, p$. Indeed, if $m|p$, then there exists n such that $p = m \cdot n$. Hence by the hypothesis on p, one has$p|m$ or $p|n$. W.ł.o.g., let $p|m$. Then by definition, there exists $k \in \mathbb{N}$ such that $m = p \cdot k$. Hence finally one has:

$$p = m \cdot n = (p \cdot k) \cdot n = p \cdot (k \cdot n)$$

and by the cancelation property, one gets $1 = k \cdot n$ (WHY), thus $k = n = 1$ (WHY). Hence conclude that $p = m \cdot n = m \cdot 1 = m$.

The implication "$\Rightarrow$": We make induction on p, and claim that $\mathcal{Q}_p \equiv \big[\big(p \text{ prime } \& \; p|(m \cdot n)\big) \Rightarrow (p|m \vee p|n)\big)\big]$ are true for all prime numbers. Indeed, first, $\mathcal{Q}_2$ asserts that if $2|(m \cdot n)$ then $2|m$ or $2|n$. By contradiction, suppose that 2 does neither divide m nor n. Then $m = 2k + 1$, $n = 2l + 1$ for some $k, l \in \mathbb{N}$, hence $m \cdot n = 2(2k \cdot l + k + l) + 1$, hence 2 doesn't divide $m \cdot n$, contradiction! Second, to prove $\mathcal{Q}_p$, suppose $\mathcal{Q}_q$ are true for all $q < p$. Let $p \mid (m \cdot n)$, and *by contradiction,* suppose that p does not divide either m or n. Hence using division with remainder, one has $m = m' \cdot p + r$, $n = n' \cdot p + s$ with $0 \leqslant r, \; s < p$. Hence on gets:

$$m \cdot n = p(p \cdot m' \cdot n' + m' + n') + r \cdot s = p \cdot k + r \cdot s, \quad \text{where } k := p \cdot m' \cdot n' + m' + n'$$

and therefore: Since $m \cdot n = p \cdot k + r \cdot s$, and p divides both $m \cdot n$ and $p \cdot k$, it follows that $p|(r \cdot s)$ (WHY). We claim that actually $1 < r, \; s$. Indeed, since p does not divide m or n, we must have $r, \; s \neq 0$ (WHY), hence $0 < r, s < p$. We claim that $r, s > 1$. Indeed, by contradiction, suppose that $r = 1$. Then $r \cdot s = s$, hence $p|(r \cdot r)$ implies $p|r$ (WHY), contradiction! The case $s = 1$ is similar. Hence $1 < r, \; s < p$, and since $p|(r \cdot s)$, by definition one has: There exists $l \in \mathbb{N}$ such that

$$p \cdot l = r \cdot s \, .$$

To reach the desired contradiction, we make induction on l. First, if $l = 1$, then $p = p \cdot l = r \cdot s$, thus contradicting the fact that p is a prime number (WHY). Next suppose that $l > 1$. Let q be any prime number dividing r, say $r = q \cdot r'$ for some $r' \in \mathbb{N}$. Then $q \leq r < p$, hence $\mathcal{Q}_q$ is true (WHY). And since q divides $r \cdot s = p \cdot l$, we must have $q|p$ of $q|l$; and since p is a prime number, and $q < p$, we finally must have $q|l$. Thus setting $l = q \cdot l'$, we get $p \cdot l = p \cdot q \cdot l' = q \cdot r' \cdot s$, hence $p \cdot q \cdot l' = q \cdot r' \cdot s$. Thus by the cancelation property, one gets $p \cdot l' = r' \cdot s$. Hence since $l' < l$ (WHY), we reached a contradiction. The Key Lemma is proved. $\square$

Coming back to the proof of assertion 3) of the Theorem, one has: Let $p_1 \dots p_r = n = q_1 \dots q_s$ be presentations of n as product of prime numbers $p_1 \leqslant \; \dots \; \leqslant p_r$ and $q_1 \leqslant \; \dots \; \leqslant q_s$. We prove that $p_r = q_s$. Indeed, let p be the maximal prime number dividing n. Then $p_r, q_s \leqslant p$ (WHY), and since $p|(p_1 \dots p_r)$, it follows that $p|p_i$ so some p_i (WHY), thus $p = p_i$ (WHY). Hence one has $p = p_i \leqslant p_r \leqslant p$, concluding that $p = p_r$. Similarly, $p = q_s$, thus $p_r = p = q_s$, as claimed. Hence if $r = 1$ or $s = 1$, or equivalently, $n = p_r$ or $n = q_s$, we are done (WHY). If $r, s > 1$, then setting $n = m \cdot p_r = m \cdot p = m \cdot q_s$, one has: $p_1 \dots p_{r-1} = m = q_1 \dots q_{s-1}$ (WHY). Thus making induction on n, we have that $m < n$. Therefore, by the induction hypothesis, one has $r - 1 = s - 1$, and $p_i = q_i$ for $1 \leqslant i \leqslant r - 1 = s - 1$ (WHY). Hence $r = s$, and $p_i = p_j$ for $1 \leqslant i \leqslant r = s$ (WHY). $\square$

Remark 2.7. There is a host of open important and fascinating problems concerning prime numbers and factorization of numbers. The problems are od simply theoretical nature, whereas other such problems are of fundamental importance for encryption and coding of information. Here is a mini-list of such questions:

1) The twin-prime Problem: Are there infinitely many prime numbers p_k such that $p_k + 2$ is a prime number as well? (Google it!)

   Example 2.8. $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, ... are pairs of twin-prime numbers.

2) Given any $n \in N$, is there a prime number p such that $n^2 \leqslant p \leqslant (n+1)^2$? More general, what can one say about the gaps between prime numbers, i.e., $p_{k+1} - p_k$ for any consecutive primes p_k, p_{k+1}? [prime gaps (Google it!)]
3) What is the minimal number of operation necessary to check whether a given natural number n is a prime number? [primality Test (Google it!)]
4) What is the minimal number of operations necessary to find a prime factor of a natural number n? [factorization problem (Google it!)]

3. The Ring of Integer Numbers $\mathbb{Z}, +, \cdot$

The deficiency of computation in the natural numbers is lacking the possibility of **making subtractions** "$m - n$" for $m, n \in \mathbb{N}$, whereas that feature would be very useful for practical and philosophical reasons; e.g. to solve very simple equations of the form $x + n = m$.

Note. One can though define subtraction partially, namely, if $k + m = n$, one can set $k :\overset{\text{def}}{=} n - m$, $m :\overset{\text{def}}{=} n - k$, but this does not completely solve the problem of subtraction (WHY).

The remedy for the lack of subtraction is to define/introduce a bigger set of numbers which, first contains $\mathbb{N}$, and second, has addition $\oplus$ and multiplication $\odot$ prolonging the ones from $\mathbb{N}$. The set of "numbers" with those properties together with $\oplus$ and $\odot$ is the

ring of integers numbers $\mathbb{Z}, +, \cdot$

The definition of the set of integer numbers $\mathbb{Z}$ is as follows: Let $\mathcal{Z} := \mathbb{N} \times \mathbb{N}$ viewed as a set, and define on $\mathcal{Z}$ the following relation: $(m, n) \sim (m', n') \overset{\text{def}}{\longleftrightarrow} m + n' = m' + n$. Intuitively, if we denote $(m\text{-}n) :\overset{\text{def}}{=} (m, n)$, then the relation $\sim$ means simply that $(m\text{-}n) = (m'\text{-}n') \overset{\text{def}}{\longleftrightarrow} m + n' = m' + n$, which makes complete sense in $\mathbb{N}$ (WHY).

Claim. *$\sim$ is an equivalence relation on $\mathcal{Z}$.*

Indeed, reflexivity $(m, n) \sim (m, n)$, and antisymmetry $(n, m) \sim (m', n')$ iff $(m', n') \sim (m, n)$ are clear (WHY). Finally, for transitivity, let $(n, m) \sim (m', n')$ & $(n', m') \sim (m'', n'')$ be given. Then $m + n' = m' + n$ & $m' + n'' = m'' + n'$ (WHY), hence $m + n' + m' + n'' = m' + n + m'' + n'$ (WHY), thus canceling $m' + n'$ we get: $m + n'' = n + m''$, i.e., $(n, m) \sim (m'', n'')$ as claimed.

Notations. We denote $\mathbb{Z} := \mathcal{Z}/\!\sim$ and call it the set of integer numbers. And for the time being, we denote the equivalence class $(m,n)/\!\sim$ of (m,n) by $(m\text{-}n) :\overset{\text{def}}{=} (m, n)/\!\sim$.

Theorem 3.1. *In the above notations, the following hold:*

1) *Defined an* addition $\oplus$ *on* $\mathbb{Z}$ *by* $(m\text{-}n) \oplus (k\text{-}l) \ :\overset{\text{def}}{=} ((m+k)\text{-}(n+l))$. *Then* $\oplus$ *is well defined, associative, commutative,* $0_{\mathbb{Z}} := (0\text{-}0)$ *is neutral element, and* $(-a) := (n\text{-}m)$ *satisfies* $a \oplus (-a) = 0_{\mathbb{Z}}$. ***Hence*** $\mathbb{Z}, \oplus$ ***is an abelian group with neutral element*** $0_{\mathbb{Z}}$.
2) *Defined a* multiplication $\odot$ *on* $\mathbb{Z}$ *by* $(m\text{-}n) \odot (k\text{-}l) \ :\overset{\text{def}}{=} ((mk+nl)\text{-}(ml+nk))$. *Then* $\odot$ *is well defined, associative, commutative,* $1_{\mathbb{Z}} := (1\text{-}0)$ *is neutral element, and has cancellation.* ***Hence*** $\mathbb{Z}, \odot$ ***is an abelian monoid with neutral element*** $1_{\mathbb{Z}}$.
3) *The multiplication* $\odot$ *is distributive w.r.t. the addition* $\oplus$, *and therefore one finally has:*

$\mathbb{Z}, \oplus, \odot$ ***is a commutative ring with*** $1_{\mathbb{Z}}$.

Moreover, the map $\imath : \mathbb{N} \to \mathbb{Z}$ *defined by* $\imath(n) :\overset{\text{def}}{=} (n\text{-}0)$ *is injective and satisfies:*

$$\imath(0) = 0_{\mathbb{Z}},\ \imath(1) = 1_{\mathbb{Z}},\ \imath(m+n) = \imath(m) \oplus \imath(n),\ \imath(m \cdot n) = \imath(m) \odot \imath(n)\ \forall\, m, n \in \mathbb{N}.$$

Terminology. $\mathbb{Z}, +, \cdot$ is called the ring of integer numbers.

Proof. To 1): We first prove that $\oplus$ is well defined. That is, we have to prove that if $(m, n) \sim (m', n')$ and $(k, l) \sim (k', l')$, then $(m\text{-}n) \oplus (k\text{-}l) = (m'\text{-}n') \oplus (k'\text{-}l')$. Equivalently, we have to show that $m + n' = m' + n$ & $k + l' = k' + l \Rightarrow (m + k, n + l) \sim (m' + k', n' + l')$ (WHY). OTOH, the latter condition is equivalent to $m + k + n' + l' = m' + k' + n + l$, and that follows by simply adding $m + n' = m' + n$ & $k + l' = k' + l$. Further, the associativity and commutativity of $\oplus$ follow instantly from the definition of $\oplus$ together with the associativity and commutativity of $+$ in $\mathbb{N}$ (HOW). Next one checks that $0_{\mathbb{Z}} := (0\text{-}0)$ is neutral element for $\oplus$, and that $(n\text{-}m)$ is the inverse of $(m\text{-}n)$ w.r.t. $\oplus$ (WHY). In particular, the inverse of $k = (k\text{-}0)$ w.r.t. the addition $\oplus$ is $-k := (0\text{-}k)$, and the inverse of $-l := (0\text{-}l)$ w.r.t. addition is $l = (l\text{-}0)$ (WHY).

To 2) As above, we first prove that $\odot$ is well defined. That is, we have to prove that if $(m,n) \sim (m',n')$ and $(k,l) \sim (k',l')$, then $(m\text{-}n) \odot (k\text{-}l) = (m'\text{-}n') \odot (k'\text{-}l')$. For that it is sufficient to show that

$$(m\text{-}n) \odot (k\text{-}l) = (m'\text{-}n') \odot (k\text{-}l), \quad \text{and} \quad (m'\text{-}n') \odot (k\text{-}l) = (m'\text{-}n') \odot (k'\text{-}l') \quad \text{(WHY)}.$$

We prove the first assertion (the second one being proven completely similarly). Hence we have to show that $m + n' = m' + n \Rightarrow (mk + nl, ml + nk) \sim (m'k + n'l, m'l + n'k)$ (WHY), or equivalently, to show that $mk + nl + m'l + n'k = ml + nk + m'k + n'l$ (WHY). On the other hand, since $m + n' = m' + n$, one has:

$$mk + nl + m'l + n'k \overset{\text{why}}{=} (m + n')k + (n + m')l \overset{\text{why}}{=} (m' + n)k + (m + n')l \overset{\text{why}}{=} m'k + nk + ml + n'l, \quad \text{done!}$$

Further, the associativity and commutativity of $\odot$ follow instantly from the definition of $\odot$ together with the associativity and commutativity of $+$ and $\cdot$ in $\mathbb{N}$ (HOW). And $1_{\mathbb{Z}} := (1\text{-}0)$ is neutral element for multiplication:

$$(m\text{-}n) \odot 1_{\mathbb{Z}} \overset{\text{why}}{=} 1_{\mathbb{Z}} \odot (m\text{-}n) \overset{\text{def}}{:=} \big((1 \cdot m + 0 \cdot n)\text{-}(0 \cdot m + 1 \cdot n)\big) = (m\text{-}n) \quad \text{(WHY)}.$$

To 3): **Ex** (use the definitions of $\oplus$ and $\odot$ and the properties of $+$ and $\cdot$ in $\mathbb{N}$).

Finally, the assertions concerning the map $\imath : \mathbb{N} \to \mathbb{Z}$ follow directly from the definition (HOW) **Ex** ... □

Remark 3.2. In the above notations one has:

a) Let $m \geqslant n$, hence $m = n + k$ for a unique $k \in \mathbb{N}$ (WHY). In particular, $(m,n) \sim (k,0)$ (WHY). Similarly, if $m \leqslant n$, then $m + l = n$ for a unique $l \in \mathbb{N}$, and if so, then $(m,n) \sim (0,l)$.

b) Moreover, $(k,0) \sim (k',0)$ iff $k = k'$ (WHY), and similarly, $(0,l) \sim (0,l')$ iff $l = l'$ (WHY).

c) Hence we conclude that the equivalence class of every (m,n), denoted $(m\text{-}n)$, equals either $(k\text{-}0)$, or $(0\text{-}l)$ for a unique $k \in \mathbb{N}$, respectively $l \in \mathbb{N}$ (WHY).

Convention. We identify every $n \in \mathbb{N}$ with $\imath(n) = (n\text{-}0) \in \mathbb{Z}$, and view $\mathbb{N}$ as subset of $\mathbb{Z}$. In particular, since by the Remark 3.2, b) above, every $(m\text{-}n) \in \mathbb{Z}$ is either of the form $(k\text{-}0)$ or of the form $(0\text{-}l)$, it follows that setting $-n := (0\text{-}n)$, one has that

$$\mathbb{Z} = \{\, -n \mid n \in \mathbb{N} \,\} \cup \{\, n \mid n \in \mathbb{N} \,\} = \{\dots, -n, \dots, -2, -1, 0, 1, 2, \dots, n, \dots\}$$

Note that with these notations one actually has:

$$(m\text{-}n) \overset{\text{why}}{=} (m\text{-}0) + (0\text{-}n) \overset{\text{why}}{=} m + (-n) \overset{\text{why}}{=} m - n \quad \text{with} \quad m, n \in \mathbb{N},$$

hence the interpretation of $(m\text{-}n)$ is compatible with the usual addition (and multiplication) in $\mathbb{Z} = \{\, -n \mid n \in \mathbb{N} \,\} \cup \{\, n \mid n \in \mathbb{N} \,\}$ as defined above (as an abstract set).

In particular, under the identification $n = (n\text{-}0)$ we make get the identifications:

$$\text{addition:} \quad 0 = 0_{\mathbb{Z}}, \qquad \text{multiplication:} \quad 1 = 1_{\mathbb{Z}}.$$

Definition 3.3. Define on $\mathbb{Z}$ the relation $a \leqslant b \overset{\text{def}}{\longleftrightarrow} a = b + l$ for some $l \in \mathbb{N}$.

Proposition 3.4. *The following hold:*

1) *The relation $\leqslant$ on $\mathbb{Z}$ is a total ordering, and for all natural numbers $m, n \in \mathbb{N}$ one has: $m \leqslant n$ in $\mathbb{N}$ iff $m \leqslant n$ in $\mathbb{Z}$.*

2) *The ordering $\leqslant$ on $\mathbb{Z}$ is compatible with the addition and the multiplication, i.e., $\forall\, a, b, c \in \mathbb{Z}$, one has: $a \leqslant b \Rightarrow a + c \leqslant b + c$, and $a \cdot c \leqslant b \cdot c$, provided $c \geqslant 0_{\mathbb{Z}}$.*

Proof. **Ex** ... □

Theorem 3.5. *The addition, multiplication, and ordering in $\mathbb{Z}$ satisfy cancellation, i.e., for all $a, b, c \in \mathbb{Z}$, the following hold:*

1) $a + c = b + c$ *iff* $a = b$, *and* $a \cdot c = b \cdot c$ *iff* $a = b$, *provided* $c \neq 0_{\mathbb{Z}}$.
2) $a + c \leqslant b + c$ *iff* $a = b$, *and* $a \leqslant b$ *iff* $a \cdot c \leqslant b \cdot c$, *provided* $c > 0_{\mathbb{Z}}$.

Proof. To 1): The assertion about $+$ is left as an exercise (use the fact that $\mathbb{Z}, +$ is a group, and prove that group satisfy the cancelation property). For the cancelation property of the multiplication, let $a = \overline{(m\text{-}n)}$ and $b = \overline{(p\text{-}q)}$. First, suppose that $c = k = \overline{(k\text{-}0)}$ for some $k \in \mathbb{N}$; in particular, since $c \neq 0_{\mathbb{Z}}$, one must have $k \neq 0$ (WHY). One has:

$$\overline{(mk\text{-}nk)} \overset{\text{why}}{=} \overline{(m\text{-}n)} \odot \overline{(k\text{-}0)} = a \cdot c = b \cdot c = \overline{(p\text{-}q)} \odot \overline{(k\text{-}0)} \overset{\text{why}}{=} \overline{(pk\text{-}qk)}\,,$$

hence $mk + qk = pk + nk$, thus $(m+q)k = (p+n)k$. Therefore, since $k \neq 0$ in $\mathbb{N}$, by the cancellation property one gets: $m + q = p + n$, thus $a = \overline{(m\text{-}n)} = \overline{(p\text{-}q)} = b$. Second, if $c = -k$ for some $k \in \mathbb{N}$, $k \neq 0$, **Ex** . . . .

To 2): Notice that by the definition of $\leqslant$ one has: If $c > 0_{\mathbb{Z}}$, then $c = \overline{(k\text{-}0)}$ for some $k \in \mathbb{N}$, $k \neq 0$. Hence in the notations from the proof of assertion 2), first case, one has: $a \cdot c \leqslant b \cdot c$ iff $\overline{(mk\text{-}nk)} \leqslant \overline{(pk\text{-}qk)}$ iff $\exists\, l \in \mathbb{N}$ such that $\overline{(mk\text{-}nk)} + \overline{(l\text{-}0)} = \overline{(pk\text{-}qk)}$ iff $mk + l + qk = pk + nk$ (WHY). Hence by the divisibility in $\mathbb{N}$, it follows that $k|l$ in $\mathbb{N}$ (WHY), hence $l = kl'$ for some $l' \in \mathbb{N}$. Hence finally get $(m + l' + q)k = (p + n)k$, thus $m + l' + q = p + n$ (WHY). Therefore, $a + l' = \overline{(m\text{-}n)} + \overline{(l'\text{-}0)} = \overline{(q\text{-}p)} = b$, thus $a \leqslant b$ (WHY). □

4. The Field of Rational Numbers $\mathbb{Q}, +, \cdot$

As in the case of natural numbers $\mathbb{N}$, the integers $\mathbb{Z}$ have the disadvantage that one cannot solve in $\mathbb{Z}$ simple linear equations, e.g., $2x + 4 = 1$, etc. Equivalently, in the ring of integers $\mathbb{Z}$ one cannot divideby arbitrary non-zero integer numbers, e.g., "$\frac{-3}{2}$" is not a number in $\mathbb{Z}$.

Note. One can though define division in $\mathbb{Z}$ partially, namely, if $a = b \cdot r$ and $r \neq 0_{\mathbb{Z}}$, one can set $b :\overset{\text{def}}{=} \frac{a}{r}$, but this does not completely solve the problem of division (WHY).

The remedy for that is to consider/define a larger set of numbers, which contains in a natural way the integers $\mathbb{Z}$, and is endowed with an addition $\oplus$ and multiplication $\odot$, which extend the ones in $\mathbb{Z}$. The set of "numbers" with those properties together with $\oplus$ and $\odot$ is the

field of rational numbers $\mathbb{Q}, +, \cdot$

The definition of the set of rational numbers $\mathbb{Q}$ is as follows: Let $\mathcal{Q} := \mathbb{Z} \times \mathbb{Z}^\bullet$ viewed as a set, where $\mathbb{Z}^\bullet = \mathbb{Z} \setminus \{0_{\mathbb{Z}}\}$ is the set of non-zero integer numbers. We define on $\mathcal{Q}$ the following relation: $(a, r) \sim (a', r') \overset{\text{def}}{\longleftrightarrow} a \cdot r' = a' \cdot r$. Intuitively, setting $\frac{a}{r} :\overset{\text{def}}{=} (a, r)/\!\sim$, the relation $\sim$ means simply that $\frac{a}{r} = \frac{a'}{r'} \overset{\text{def}}{\longleftrightarrow} a \cdot r' = a' \cdot r$, which makes complete sense in $\mathbb{Z}$ (WHY).

Claim. $\sim$ *is an equivalence relation on* $\mathcal{Q}$.

Indeed, reflexivity $(a, r) \sim (a, r)$, and antisymmetry $(a, r) \sim (a', r')$ iff $(a', r') \sim (a, r)$ are clear (WHY). Finally, for transitivity, let $(a, r) \sim (a', r')$ & $(a', r') \sim (a'', r'')$ be given. Then $a \cdot r' = a' \cdot r$ & $a' \cdot r'' = a'' \cdot r'$ (WHY), hence $a \cdot r' \cdot a' \cdot r'' = a' \cdot r \cdot a'' \cdot r'$ (WHY). Hence since $r, r', r'' \neq 0_{\mathbb{Z}}$, one has: First, if $a' = 0_{\mathbb{Z}}$, then $a = a'' = 0_{\mathbb{Z}}$ (WHY), hence $a \cdot r'' = a'' \cdot r$ (WHY); second, if $a' \neq 0_{\mathbb{Z}}$, then $a' \cdot r' \neq 0_{\mathbb{Z}}$ (WHY), hence one has cancellation by $a' \cdot r'$ in $\mathbb{Z}$ (WHY), and one gets again $a \cdot r'' = a'' \cdot r$ (WHY); thus finally one always has $a \cdot r'' = a'' \cdot r$, as claimed.

Notations. We denote $\mathbb{Q} := \mathcal{Q}/\!\sim$ and call it the set of rational numbers. And for the time being, we denote the equivalence class $(a,r)/\!\sim$ of (a,r) by $\frac{a}{r} :\overset{\text{def}}{=} (a,r)/\!\sim$.

Theorem 4.1. *In the above notations, the following hold:*

1) *Define an* addition $\oplus$ *on* $\mathbb{Q}$ *by* $\frac{m}{n} \oplus \frac{b}{s} :\overset{\text{def}}{=} \frac{as+br}{rs}$. *Then* $\oplus$ *is well defined, associative, commutative, has neutral element* $0_{\mathbb{Q}} := \frac{0}{1}$, *and* $(-x) := \frac{-a}{r}$ *is the inverse of* $x = \frac{a}{r}$ *w.r.t.* $\oplus$. ***Hence*** $\mathbb{Q}, \oplus$ ***is an abelian group with neutral element*** $0_{\mathbb{Q}}$**.**
2) *Define a* multiplication $\odot$ *on* $\mathbb{Q}$ *by* $\frac{a}{r} \odot \frac{b}{s} :\overset{\text{def}}{=} \frac{ab}{rs}$. *Then* $\odot$ *is well defined, associative, commutative, has neutral element* $1_{\mathbb{Q}} := \frac{1}{1}$, *and each* $x = \frac{a}{x} \neq 0_{\mathbb{Q}}$ *has* $x^{-1} := \frac{r}{a}$ *as an inverse w.r.t.* $\oplus$. ***Hence*** $\mathbb{Q}^{\bullet}, \odot$ ***is an abelian group with neutral element*** $1_{\mathbb{Q}}$**.**
3) *The multiplication* $\odot$ *is distributive w.r.t. the addition* $\oplus$, *and therefore one finally has:*

$$\mathbb{Q}, \oplus, \odot \textit{ is a field.}$$

Moreover, the map $\imath : \mathbb{Z} \to \mathbb{Q}$ *defined by* $\imath(a) :\overset{\text{def}}{=} \frac{a}{1}$ *is injective and satisfies:*

$$\imath(0_{\mathbb{Z}}) = 0_{\mathbb{Q}},\ \imath(1_{\mathbb{Z}}) = 1_{\mathbb{Q}},\ \imath(a+b) = \imath(a) \oplus \imath(b),\ \imath(a \cdot b) = \imath(a) \odot \imath(b)\ \forall\, a, b \in \mathbb{Z}.$$

Terminology. $\mathbb{Q}, +, \cdot$ is called the *field of rational numbers.*

Proof. To 1): We first prove that $\oplus$ is well defined. That is, we have to prove that if $(a, r) \sim (a', r')$ and $(b, s) \sim (b', s')$, then $\frac{a}{r} \oplus \frac{b}{s} = \frac{a'}{r'} \oplus \frac{b'}{s'}$. Equivalently, we have to show that

$$a r' = a' r \ \ \& \ \ b s' = b' s \ \ \Rightarrow \ \ (as + br, rs) \sim (a's' + b'r', r's') \ \ \text{(WHY)}.$$

OTOH, the latter condition is equivalent to $(as + br)r's' = (a's' + b'r')rs$, and that follows easily, because:

$$(as + br)r's' \overset{\text{why}}{=} (ar')ss' + (bs')rr' \overset{\text{why}}{=} (a'r)ss' + (b's)rr' \overset{\text{why}}{=} (a's' + b's')rs$$

Further, the associativity and commutativity of $\oplus$ follow instantly from the definition of $\oplus$ together with the associativity and commutativity of $+$ in $\mathbb{Z}$ (HOW). Next one checks that $0_{\mathbb{Q}} := \frac{0}{1}$ is neutral element for $\oplus$, and that $\frac{-a}{r}$ is the inverse of $\frac{a}{r}$ w.r.t. $\oplus$ (WHY).

To 2) As above, we first prove that $\odot$ is well defined. That is, we have to prove that if $ar' = a'r$ & $bs' = b's \Rightarrow (ab, rs) \sim (a'b', r's')$ (WHY), or equivalently, that $abr's' = a'b'rs$, and that is clear (WHY). Further, the associativity and commutativity of $\odot$ follow instantly from the definition of $\odot$ together with the associativity and commutativity of $+$ and $\cdot$ in $\mathbb{N}$ (HOW). And $1_{\mathbb{Q}} := \frac{1_{\mathbb{Z}}}{1_{\mathbb{Z}}}$ is neutral element for multiplication (WHY).

To 3): **Ex** (use the definitions of $\oplus$ and $\odot$ and the properties of $+$ and $\cdot$ in $\mathbb{Z}$).

Finally, the assertions concerning the map $\imath : \mathbb{Z} \to \mathbb{Q}$ follow directly from the definition (HOW) **Ex** ... □

Convention. We identify $a \in \mathbb{Z}$ with $\imath(a) = \frac{a}{1} \in \mathbb{Q}$, and view $\mathbb{Z}$ as subset of $\mathbb{Q}$. In particular, since $\mathbb{N}$ is identified with all the integers of the form $(n\text{-}0)$, and $\mathbb{N}$ is viewed as a subset of $\mathbb{Z}$, we finally has canonical inclusions

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \quad \textit{by identifying/setting} \quad a = \frac{a}{1} \ \ \textit{for } a \in \mathbb{Z}\,.$$

Moreover, the inclusions above are compatible with addition and multiplication, and identify

$$\text{addition:} \quad 0 = 0_{\mathbb{Z}} = 0_{\mathbb{Q}}, \qquad \text{multiplication:} \quad 1 = 1_{\mathbb{Z}} = 1_{\mathbb{Q}}.$$

Remark 4.2. Let $x = \frac{a}{r} \in \mathbb{Q}$, $x \neq 0_{\mathbb{Q}}$, be a fixed rational number, hence $a \neq 0$. TFH:

a) There are unique $a_0, r_0 \in \mathbb{N}_{>0}$ which are relatively prime, i.e., the only common divisor of a_0, r_0 is 1, such that either $\frac{a}{r} = \frac{a_0}{r_0}$ or $\frac{a}{r} = \frac{-a_0}{r_0}$.
b) The following are equivalent: (i) $\frac{a}{r} = \frac{a_0}{r_0}$; (ii) either $a, r < 0_{\mathbb{Z}}$ or $a, r > 0_{\mathbb{Z}}$ in $\mathbb{Z}$.

Definition 4.3. Define on $\mathbb{Q}$ the relation $x \leqslant y \overset{\text{def}}{\longleftrightarrow}$ either $x = y$ or $y - x = \frac{a}{r}$ satisfies the equivalent conditions (i), (ii) from the Remark 4.2, b) above.

Proposition 4.4. *The relation $\leqslant$ on $\mathbb{Q}$ is a total ordering, and the following hold:*

1) *For all integer numbers $a, b \in \mathbb{Z}$ one has: $a \leqslant b$ in $\mathbb{Z}$ iff $a \leqslant b$ in $\mathbb{Q}$.*
2) *The ordering $\leqslant$ on $\mathbb{Q}$ is compatible with the addition and the multiplication, i.e., $\forall\, x, y, z \in \mathbb{Q}$, one has: $x \leqslant y \Rightarrow x + z \leqslant y + z$, and $x \cdot z \leqslant y \cdot z$, provided $z \geqslant 0_{\mathbb{Q}}$.*

Proof. We prove that $\leqslant$ is a total ordering: Let $x, y \in \mathbb{Q}$, $x \neq y$ be given. Setting $x - y = \frac{a}{r}$, one has $a, r \neq 0_{\mathbb{Z}}$ (WHY), and further: First, if $a, r < 0_{\mathbb{Z}}$ or $a, r > 0_{\mathbb{Z}}$, then by definition, $x > y$. Second, if either (i) $a < 0_{\mathbb{Z}}, r > 0_{\mathbb{Z}}$ or (ii) $a > 0_{\mathbb{Z}}, r < 0_{\mathbb{Z}}$, then either (i) $-a, r > 0_{\mathbb{Z}}$ or (ii) $-a, r < 0_{\mathbb{Z}}$, hence in both cases $x < y$ (WHY). The proof of assertions 1), 2) is left as **Ex** . . . ☐

Theorem 4.5. *The addition, multiplication, and ordering in $\mathbb{Q}$ satisfy cancellation, i.e.,*

1) *$\forall\, x, y, z \in \mathbb{Q}$ one has: $x + z = y + z$ iff $x = y$; $x \cdot z = y \cdot z$ iff $x = y$, provided $z \neq 0_{\mathbb{Q}}$.*
2) *$\forall\, x, y, z \in \mathbb{Q}$ one has: $x + z \leqslant y + z$ iff $x = y$; $x \leqslant y$ iff $x \cdot z \leqslant y \cdot z$, provided $z > 0_{\mathbb{Q}}$.*

Proof. To 1) **Ex** (use the fact that $\mathbb{Q}, +$ and $\mathbb{Q}^{\times} := \{x \in \mathbb{Q} \mid x \neq 0_{\mathbb{Q}}\}$ endowed with $\cdot$ are groups).
To 2): First, for all $z \in \mathbb{Q}$, $x \neq 0_{\mathbb{Q}}$, one has $z^2 > 0_{\mathbb{Q}}$ and $z > 0_{\mathbb{Q}}$ iff $z^{-1} > 0_{\mathbb{Q}}$ (WHY). Thus finally one has: $x \cdot z \leqslant y \cdot z$ and $z > 0_{\mathbb{Q}}$ imply: $x \cdot z \cdot z^{-1} \leqslant y \cdot z \cdot z^{-1}$ (WHY), thus $x \leqslant y$ (WHY). ☐

Email address: pop@math.upenn.edu
URL: http://math.penn.edu/~pop