MATH ABC (FALL 2021)

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

Axiomatic point of view for sets

- All entities are sets.
- 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 $X \in A$"].

NOTE: The intuitive or naive point of view that "the sets are all the collections of elements sharing some common property" is **not right**, because it leads to logical contradictions:

(!) Consider all the naive sets X such that $X \notin X$ (that is, X is not an element of itself). Call such a naive set a *normal set,* respectively, if X is a naive set with $X \in X$, call it *abnormal.* Now let $\mathcal{X}$ be the collection of all the normal sets, that is $\mathcal{X}$ is the naive set of all the sets X having the common property $p(X)$, where $p(X)$ means $X \notin X$. *Then the naive set $\mathcal{X}$ is not normal, and not abnormal.* (WHY) Hence the naive definition of a set leads to logical contradictions!

Nevertheless, 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! In particular, from the 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:

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

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 Normality***
For every set A there exists $X \in A$ such that A and X have no common elements.

As a consequence one has:

Proposition 1.9. *Every set A is normal, i.e., $A \notin A$.*

Proof. First 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., $A \notin A$, as claimed.

Second, 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 $X = A$, that is, only the case (ii), i.e., $X = B$ is possible. Hence the sets $X = B$ and $\{A, B\}$ cannot have any elements in common, thus implying that $A \notin B$ (WHY). □

5. ***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 1.10. 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 1.11. 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 1.12. *Let $\mathcal{F} = \{A \mid A \in \mathcal{F}\}$ be a set. Then $\{X \mid \forall\ A \in \mathcal{F}$ one has $X \in A\}$ is a set, called the intersection of the sets $A \in \mathcal{F}$.*

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

Remark 1.13. 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 1.14. Let A, B, C and $A_1, \ldots, A_n$ be sets. Then $A \cap B \cap C$ and $\cap_{i=1}^n A_i$ are sets.

Definition 1.15. 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 $A \triangle B := (A\backslash B) \cup (B\backslash A)$ 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 1.16. Show that $A' \cap \left(\complement_A A'\right) = \emptyset$ and $A' \cup \left(\complement_A A'\right) = A$.

Definition 1.17. For any set A, $s(A) := A \cup \{A\}$ is a set (WHY), called the successor of A.

Example 1.18. Let $A = \emptyset$. Then $s(\emptyset) = \{\emptyset\}$, $s\Big(s(\emptyset)\Big) = s(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ (WHY), etc.

Ex 1.19. Let A, B be sets with $A \subset B$ and $s(A) = s(B)$. Show that $A = B$.

Remark 1.20. 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).
- $X_0 := A \subset X_1 := s(X_0) \subset X_2 := s(X_1) \subset X_3 := s(X_2) \subset \ldots$ 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 1.21. 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 $A_n := \{X_0, X_1, \dots, X_n\}$ [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 1.22. 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 1.23. *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 1.24. 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 $\mathrm{pr}_A(R) = A$ (WHY).

Definition 1.25. 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 1.26. 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 1.27. 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 1.28. 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 1.29. 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 $\mathrm{id}_A : A \to A$ define by $\mathrm{id}_A(x) = x$ for all $x \in A$.

Remark 1.30. 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 1.31. Let A, B be sets. Then $\mathrm{Maps}(A,B) := \{f \mid f : A \to B \text{ map}\}$ 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 1.32. 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 $f(A) = B$.
3) f is called bijective, if f is both injective and surjective.

Ex 1.33. Let $f\colon A \to B$ 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: $g\Big(f(x)\Big) = x$ for all $x \in A$, and $f\Big(g(y)\Big) = y$ 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 $f\colon A \to B$, $g\colon B \to C$ be maps. Define $g \circ f\colon A \to C$ by the rule $(g \circ f)(x) := g\Big(f(x)\Big)$. 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.*
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.*

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. To 2): **Ex** . . . □

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

Theorem 1.38. *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, $A_\emptyset = \{\emptyset\}, A_{s(\emptyset} = \{\emptyset, \{\emptyset\}\}, A_{s(s(\emptyset))}, \dots$ 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, it follows that $A_0 = C_0 = B_0$ (WHY). Thus we conclude that the set $\mathbb{N} := A_0$ is the unique set satisfying condition i), ii), iii). □

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

Remark 1.39. 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 1.40. (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 1.41. (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* $(\mathcal{Q}_0 \,\&\, \dots \,\&\, \mathcal{Q}_n) \Rightarrow \mathcal{Q}_{s(n)}$ *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 1.42. *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 1.43. 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 there are no injective maps $f : B \to A$.

Definition 1.44. 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 1.45. 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 1.46. 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 1.47. *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}. □

Concerning infinite sets, the hollowing holds:

Proposition 1.48. *A is infinite iff $|\mathbb{N}| \leqslant |A|$, i.e., there exists an injective map $f : \mathbb{N} \to A$.*

Proof. The implication "⇐" 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 "⇒" 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 1.49. *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) $\Rightarrow$ iii) is similar, **Ex** . . .

To i) $\Rightarrow$ 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 1.47 above.

To ii) $\Rightarrow$ 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 1.50. 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 $\mathcal{P}(A \times A)$ (WHY).

Example 1.51. 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 1.52. 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 1.53. 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 $x \in A$.
   - ii) $\sim$ is symmetric, i.e., $x \sim y \Rightarrow y \sim x$.
   - 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 1.54. 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?

Definition 1.55. 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 1.56. 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 1.57. *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 $\mathrm{pr}_1^{-1}(x) = \{(x, x') \,|\, x \sim x'\}$ for every $x \in A$ (WHY), hence a subset of R (WHY). OTOH, $\widehat{x} = \mathrm{pr}_2(\{(x, x') \,|\, x \sim x'\})$ (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** . . . □

Order relations or (partial) Ordering

Definition 1.58. 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 $x < y \overset{\text{def}}{\longleftrightarrow} y > x$.

Definition 1.59. Let $\leqslant$ be an ordering on A, and $B \subset A$ be a non-empty subset.

a) An element $y_B \in B$, if it exists, is called a minimum of B, if $y_B \leqslant y \;\forall\, y \in B$.
Define correspondingly a maximum $y^B \in B$ of B, provided it exists.
Notation. $\min(B)$, 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 1.60. 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 1.61. In the above notations, prove/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 holds 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 holds for supremum.

Ex 1.62. 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 1.63. 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 1.64. 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.

---

9. ***Axiom of Choice***
   Given any non-empty set A, one can choose an element $X \in A$.

Remark 1.65. 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 the Axiom of Choice is denoted (ZFC). On the other hand, it turns out that there are several equivalent formulations of (ZFC), e.g. one has:

Theorem 1.66. *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 $\max(A)$ exists.*

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:*

$$m \leqslant n \ \ \Rightarrow \ \ m+k \leqslant n+k,\ \ m\cdot k \leqslant n\cdot k.$$

2) *The ordering $\leqslant$ is a total ordering, and moreover, a well ordering of $\mathbb{N}$.*

Proof. To 1: Induction on k: Step 1. $\mathcal{P}_0$: $m \leq n \Rightarrow m+0 \leqslant n+0\, m \cdot k \leqslant n \cdot 0$ 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 $\mathcal{P}_n \equiv \big(\forall\, m \in \mathbb{N},$ one has $m \leq n$ or $n \leq m\big)$ 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 $m \leq n$, 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:

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

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) $\big(\mathcal{P}_0,\dots,\mathcal{P}_n\big)\Rightarrow\mathcal{P}_{s(n)}$. □

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 $r_{i-1}=q_ir_i+r_{i+1}=q_ir_i$; 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 for all* $m,n\in\mathbb{N}$ *one has:*

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

Proof. (of the Key Lemma) The implication "⇐": 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 "⇒": 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, hence $m\cdot n=2(2k\cdot l+k+l)+1$, hence 2 does not divide $m\cdot n$, contradiction! Second, to prove $\mathcal{Q}_p$, suppose that $\mathcal{Q}_q$ 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. □

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). □

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:*

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

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:

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

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 $a = (m\text{-}n)$ and $b = (p\text{-}q)$. First, suppose that $c = k = (k\text{-}0)$ for some $k \in \mathbb{N}$; in particular, since $c \neq 0_{\mathbb{Z}}$, one must have $k \neq 0$ (WHY). One has:

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

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 $a = (m\text{-}n) = (p\text{-}q) = b$. 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 $c = (k\text{-}0)$ 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 $(mk\text{-}nk) \leqslant (pk\text{-}qk)$ iff $\exists\, l \in \mathbb{N}$ such that $(mk\text{-}nk) + (l\text{-}0) = (pk\text{-}qk)$ 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, $a + l' = (m\text{-}n) + (l'\text{-}0) = (q\text{-}p) = b$, 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, that reduces to the fact that in the ring of integers $\mathbb{Z}$ one cannot divide by 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:*

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

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 $a\,r' = a'\,r$ & $b\,s' = b'\,s \Rightarrow (ab, rs) \sim (a'b', r's')$ (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 every $a \in \mathbb{Z}$ 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

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

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). □

5. Composition laws & Basic algebraic structures

5.1. Basic definitions/Facts.

Definition 5.1. A (binary) composition law on a set $X \neq \emptyset$ is any map $\psi : A \times X \to X$.
Notation. Usually, $\psi(x, y)$ is denoted by $x * y$, or $x \circ y$, or $x \cdot y$, etc. [read "x composed with y"].

Definition 5.2. Let $*$ be a composition law on X. We says that $*$ satisfies/has:
- associativity, if $(x * y) * z = x * (y * z)\ \forall\, x, y, z \in X$.
- commutativity, if $x * y = y * x\ \forall\, x, y \in X$.
- neutral element $e \in X$, if $x * e = x = e * x\ \forall\, x \in X$.
- Suppose that $*$ has a neutral element $e \in X$. We say that $x' \in X$ is an inverse of $x \in X$ (w.r.t. $*$), if $x * x' = e = x' * x$. We say that $x \in X$ is invertible, if x has an inverse $x' \in X$.

Proposition 5.3. *Let $*$ be a composition law on X. TFH:*
1) If $e, e' \in X$ are neutral elements, then $e = e'$ (WHY).
2) If $*$ is associative, and $x', x'' \in X$ are inverse elements of x w.r.t. $*$, then $x' = x''$.

Proof. To 1): One has $e' \overset{\text{why}}{=} e' * e \overset{\text{why}}{=} e$. To 2): One has: $x' \overset{\text{why}}{=} x' * e \overset{\text{why}}{=} x' * (x * x'') \overset{\text{why}}{=} (x' * x) * x'' \overset{\text{why}}{=} x''$. □

Definition 5.4. Let $X, *$ be a set endowed with a composition law.
1) $X, *$ is called a (commutative) monoid, if $*$ is associative (and commutative), and has a neutral element e_X.
2) $X, *$ is called a (commutative) group, if $X, *$ is a (commutative) monoid, and every $x \in X$ has an inverse w.r.t. $*$.

Example 5.5.
a) $+$ and $\cdot$ are composition laws on $\mathbb{N}$, and $\mathbb{N}, +$ and $\mathbb{N}, \cdot$ are commutative monoids (WHY). What are neutral elements and the investible elements in $\mathbb{N}, +$ and $\mathbb{N}, \cdot$?
b) Let $X := \mathcal{P}(A)$ be the power set of a given set A. Then $X, \cap$ and $X, \cup$ are commutative monoids (WHY). What are neutral, rest. invertible elements in these monoids, respectively?
(!) Moreover, X endowed with the symmetric difference $A \triangle B \overset{\text{def}}{:=} (A \backslash B) \cup (B \backslash A)$ is a commutative group (WHY).
c) The difference $a * b \overset{\text{def}}{:=} a - b$ is a composition law on $\mathbb{Z}$, which is not associative, nor commutative (WHY). Does $-$ have a neutral element?
d) Let $\leqslant$ be a total ordering on a set X. Then $x * y \overset{\text{def}}{:=} \min(x, y)$ and $x \circ y := \max(x.y)$ are associative and commutative (WHY). Do these composition laws have neutral elements?

3) Let X be a non-empty set. Then $\mathrm{Bij}(X) :\stackrel{\text{def}}{=} \{f \mid f : X \to X \text{ bijective}\} \subset \mathrm{Maps}(X)$ consists of the precisely invertible elements in the monoid $\mathrm{Maps}(X), \circ$ (WHY). In particular, $\mathrm{Bij}(X), \circ$ is a group (WHY), which is non-commutative if $|X| > 2$ (WHY).

(•) **The permutation group S_n.** If $X = \{1, \ldots, n\}$, one sets $S_n :\stackrel{\text{def}}{=} \mathrm{Bij}(X), \circ$ and calls it the permutation group of n elements. The elements $\sigma \in S_n$ are presented in the form:

$$\sigma := \begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix}, \quad i_k = \sigma(k) \ \forall\ 1 \leqslant k \leqslant n.$$

Definition 5.6. A (commutative) ring is a set R endowed with two composition laws, the addition $+$, and the multiplication $\cdot$ satisfying the following:

i) $R, +$ is a commutative group, i.e., $+$ is associative, commutative, has a neutral element, denoted 0_R, called the zero (element) of R, and every $x \in R$ has an an inverse w.r.t. $+$, called additive inverse of x, denoted $-x$.

ii) $R, \cdot$ is a (commutative) monoid, with neutral element denoted 1_R, called the unit element of R. The invertible elements w.r.t. $\cdot$ are called units of R, and are denoted $R^\times$.

iii) The multiplication $\cdot$ is distributive w.r.t. addition $+$, i.e., $\forall\, x, y, z \in R$ one has:

$$z \cdot (x + y) = z \cdot x + z \cdot y, \quad (x + y) \cdot z = x \cdot z + y \cdot z$$

1) A ring R is called a domain, if $0_R \neq 1_R$, R is commutative, and $\cdot$ has *cancellation,* i.e., $\forall\, x, y, z \in R$, $z \neq 0_R$ one has: $x \cdot z = y \cdot z \Rightarrow x = y$.

2) A ring $R, +, \cdot$ is called a skew field, if $1 \neq 0_R$, and every $x \in R$, $x \neq 0_R$ is invertible w.r.t. multiplication. Commutative skew fields are called simply fields.

Example 5.7 (**NOTE:** The rings & (skew) fields below will be "officially" defined later)**.**

a) $\mathbb{Z}, +, \cdot$ is a domain, and $\mathbb{Z}^\times = \{\pm 1\}$ (WHY).

b) Given a commutative ring R, e.g. $R = \mathbb{Z}$, the rings of polynomials $R[t]$ in the variable t with coefficients in R is a (commutative) ring. What are $0_{R[t]}$ and $1_{R[t]}$? What is $R[t]^\times$?

c) The set $\mathcal{M}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ of 2×2 matrices over $\mathbb{Z}$ endowed with addition and multiplication of matrices is a *non-commutative* ring (WHY). What is $\mathcal{M}_2(\mathbb{Z})^\times$?

b) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, are fields, and the Hamiltonian quaternions $\mathbb{H}$ is a skew field. Google it!

Definition 5.8. (**Computation rules in rings**)
Let $R, +, \cdot$ be a ring with 0_R and 1_R. For $n \in \mathbb{N}$, thus $-n, n \in \mathbb{Z}$, and $r \in R$, define:

a) $0\, r := 0_R$, and inductively: $(n + 1)r := (nr) + r$, $-(n + 1)r := n(-r) + (-r)$.

b) $r^1 := r$, and inductively $r^{n+1} := r^n \cdot r$.

(!) Note that setting $r^0 := 1_R$ is trickier; it is OK to set $r^0 = 1_R$ if $r \in R^\times$, but else . . .

Proposition 5.9 (Computation rules in rings). *Ler $R, +, \cdot$ be a ring. TFH:*

1) $0_R \cdot x = 0_R = x \cdot 0_R$, $(-1_R) \cdot x = -x = x \cdot (-1_R)$ *for all* $x \in R$. *Hence* $R = \{0_R\}$ *iff* $0_R = 1_R$.

2) $(\sum_{i=1}^m a_i)(\sum_{j=1}^n b_j) = \sum_{i,j} a_i b_j$, $a^m \cdot a^n = a^{m+n}$ *and* $(a^n)^m = a^{mn}$ $\forall\, a_i, b_j, a \in R$, $m, n \in \mathbb{N}_{>0}$.

3) *Suppose that* $a \cdot b = b \cdot a$ *for some* $a, b \in R$. *Then* $(a \cdot b)^m = a^m \cdot b^m$ *and* $a^m \cdot b^n = b^n \cdot a^m$ *and one has the* ***binomial formula****:* $(a + b)^n = a^n + \sum_{k=1}^{n-1} \binom{n}{k} a^{n-k} b^k + b^n$ *for* $n \in \mathbb{N}_{>0}$

Proof. To 1): $0_R \cdot x \overset{\text{why}}{=} (0_R + 0_R) \cdot x \overset{\text{why}}{=} 0_R \cdot x + 0_R \cdot x$, hence $0_R \cdot x + (-0_R \cdot x) = (0_R \cdot x + 0_R \cdot x) + (-0_R \cdot x)$, thus $0_R = 0_R \cdot x$ (WHY), etc. Further, $0_R = (1_R - 1_R) \cdot x = x + (-1_R) \cdot x$, hence $(-1_R) \cdot x = -x$ (WHY), etc.
To 2): **Ex** (make double induction on m, n, etc.) To 3): **Ex** (make induction on n, and use the binomial identity $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ —which itself can be proved either directly, or by induction (HOW) □

There are important procedures which lead to/produce new algebraic structures involving existing ones. We describe below are three such important constructions.

5.1.1. **Monoids/groups/rings of functions.**

Let $\cdot$ be a composition law on a non-empty set T, and $\mathrm{Maps}(X, T)$ be the set of maps $f : X \to T$. Define on $\mathrm{Maps}(X, T)$ the composition law:

$$(f \circ g)(x) :\overset{\text{def}}{=} \Big(f(x)\Big) \cdot \Big(g(x)\Big), \qquad \forall\, x \in X$$

called the composition law (induced by $\cdot$) *on the T-valued maps.* The following hold:

(i) $\circ$ is associative iff $\cdot$ is so (WHY).

(ii) $\circ$ is commutative iff $\cdot$ is so (WHY).

(iii) $\circ$ has a neutral element $e_\circ$ iff $\cdot$ has neutral element, say $e \in T$, and if so, the constant e-map $f_e : X \to T$, $f_e(x) = e$ is the neutral element of $\circ$ (WHY).

(iv) $f \in \mathrm{Maps}(X, T)$ has an inverse w.r.t. $\circ$ iff all $t \in f(X) \subset T$ have inverse elements in T. If so, then $g\colon X \to T$, $g(x) := \Big(\text{inverse of } t = f(x) \text{ in } T\Big)$ is the inverse of f w.r.t. $\circ$ (WHY).

Proposition 5.10. *In the above notation, for X non-empty, the following hold:*

1) *Let T endowed with a composition law $\cdot$ be given. Then $\mathrm{Maps}(X, T), \circ$ is an (abelian) monoid / group iff $T, \cdot$ is an (abelian) monoid / group.*
If so, $\mathrm{Maps}(X, T), \circ$ is called the monoid / group of T-valued functions on X.

2) *Let R endowed with two composition laws $+, \cdot$ be given. Then $R, +, \cdot$ is a (commutative) [non-trivial] ring iff $\mathrm{Maps}(X, R), \oplus, \circ$ is a (commutative) [non-trivial] ring.*
If so, $\mathrm{Maps}(X, T), \oplus, \circ$ is called the ring of T-valued functions on X.

Proof. **Ex** . . . □

NOTE. One has that R is the *trivial ring* iff $R = \{0_R\}$ iff $0_R = 1_R$ iff $\mathrm{Maps}(X, R)$ is the trivial ring (WHY). Further, if R is non-trivial, and $|X| > 1$, then there are $f, g \in \mathrm{Maps}(X, R)$ such that $f, g \neq 0_{\mathrm{Maps}(X,R)}$ and with $f \cdot g = 0_{\mathrm{Maps}(X,R)}$ (WHY).

Conclude: *If R is a (skew) field, and $|X| > 1$, then $\mathrm{Maps}(X, R)$ is not a (skew) field* (WHY).

Remark 5.11. An important case of the above situation is when $X = \mathbb{N}$. In this case, the functions $f : \mathbb{N} \to T$ are called sequences with values in T, or T-valued sequences. The usual notation for sequences is $\boldsymbol{a} := (a_n)_n$ where $\boldsymbol{a} : \mathbb{N} \to T$, and $a_n := \boldsymbol{a}(n)$. We denote by $\mathcal{S}(T) := \mathrm{Maps}(\mathbb{N}, T)$ the set of all the T-valued sequences, an notice:

a) If $T, \cdot$ is an (abelian) monoid/group, then $\mathcal{S}(T)$ is an (abelian) monoid/group w.r.t. $(a_n)_n \cdot (b_n)_n :\overset{\text{def}}{=} (a_n \cdot b_n)_n$. What is $e_{\mathcal{S}(T)}$? Which $(a_n)_n$ are invertible in $\mathcal{S}(T)$?

b) If $R, +, \cdot$ is a (commutative) ring, then $\mathcal{S}(R)$ is a (commutative) ring w.r.t. the addition $(a_n)_n + (b_n)_n :\overset{\text{def}}{=} (a_n + b_n)_n$, and multiplication $(a_n)_n \cdot (b_n)_n :\overset{\text{def}}{=} (a_n \cdot b_n)_n$.

Describe: $0_{\mathcal{S}(R)}$, $1_{\mathcal{S}(R)}$, $-(a_n)_n$, which $(a_n)_n$ are invertible w.r.t. multiplication?

5.1.2. **Products of monoids/groups/rings.**

Let $T_1, *_1$ and $T_2, *_2$ be sets with composition laws, and endow $T = T_1 \times T_2$ with the coordinate-wise composition law $*$ defined by $(x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$. Then:

(i) $*$ is associative iff $*_1$ and $*_2$ are so (WHY).

(ii) $*$ is commutative iff $*_1$ and $*_2$ are so (WHY).

(iii) $*$ has neutral element e iff $*_1$ and $*_2$ have neutral elements e_1, e_2. If so, $e = (e_1, e_2)$ (WHY).

(iv) (x_1, x_2) is invertible w.r.t. $*$ iff x_1 and x_2 have inverse elements, say x_1' and x_2' w.r.t. $*_1$ and $*_2$. If so, $x' = (x_1', x_2')$ is the inverse of $x = (x_1, x_2)$ w.r.t. $*$ (WHY).

Proposition 5.12. *In the above notation, the following hold:*

1) *Let $T_1, *_1$ and $T_2, *_2$ be sets endowed with composition laws and $T := T_1 \times T_2$ be endowed with the coordinate wise composition law $*$. Then $T_1, *_1$ and $T_2, *_2$ are (abelian) monoids/groups iff $T, *$ is an (abelian) monoid/group.*
If so, T is called the product of the monoids/groups T_1 and T_2.

2) *Let R_1 and R_2 each endowed with two composition laws be given, and $R = R_1 \times R_1$ be endowed with the two resulting coordinate wise composition laws. Then R_1 and R_2 are (commutative) rings iff R is a (commutative) ring.*
If so, R is called the product of R_1 and R_2.

Proof. **Ex** . . . □

NOTE. In the above context, R is the *trivial ring* iff $R = \{0_R\}$ iff $R_1 = \{0_{R_1}\}$, $R_2 = \{0_{R_2}\}$ iff R_1 and R_2 are both trivial (WHY). In particular, if R_1, R_2 are both nontrivial, then R contains elements $x, y \neq 0_R$ whose product is 0_R (WHY).

Conclude: *If R_1, R_2 are (skew) fields, then $R_1 \times R_2$ is not a (skew) field* (WHY).

5.1.3. **The ring of R-valued series.**

The series are quite ubiquitous in science and everyday life. One should though distinguish between the *formal series* $\sum(R)$ defined over an arbitrary commutative ring R, which are in bijection with *sequences* $\mathcal{S}(R)$, but are subject to other computation rules, and the numerical value (that is, the number) which is attached to/defined by "convergent series" series. See e.g. the examples below; this will be discussed in detail later, after defining convergence of sequences and series. Here and for the moment we discuss the *formal series* only.

Definition 5.13. Let R be an arbitrary commutative ring.

1) For a sequence $(a_n)_n \in \mathcal{S}(R)$, the symbol $\boldsymbol{\sigma} = \Sigma_n a_n$ is called the (formal) series defined by $(a_n)_n$, and a_n is called the n^{th} term or coefficient of $\Sigma_n a_n$.

Notation. Let $\sum(R) := \{\Sigma_n a_n \,|\, a_n \in R\}$ be the set of all the formal series defined over R.

2) Define in $\sum(R)$ the addition $+$, multiplication $\cdot$ and multiplication by $a \in R$ as follows:

a) $(\Sigma_n a_n) + (\Sigma_n b_n) :\overset{\text{def}}{=} \Sigma_n c_n$ where $c_n :\overset{\text{def}}{=} a_n + b_n$.

b) $(\Sigma_n a_n) \cdot (\Sigma_n b_n) :\overset{\text{def}}{=} \Sigma_n c_n$, where $c_n :\overset{\text{def}}{=} \sum_{i+j=n} a_i \cdot b_j$.

c) $a \cdot (\Sigma_n a_n) :\overset{\text{def}}{=} \Sigma_n a a_n$.

Remark 5.14. Recall that for finite sums $a := \sum_{i=1}^{m} a_i$, $b := \sum_{j=1}^{n}$ of elements of R one has: $a \cdot b = \sum_{i,j} a_i \cdot b_j$. This could be written as $a \cdot b = \sum_k c_k$, where $c_k = \sum_{i+j=k} a_i \cdot b_j$ (WHY). Hence the multiplication rules of (formal) series given at b), c) above extend—in a precise sense—the usual multiplication rules from rings.

Examples 5.15. Here are a few examples:

a) Every real number $a \geqslant 0$ has a decimal expansion: $a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n} + \ldots$

The formal series here is $\boldsymbol{\sigma} :\overset{\text{def}}{=} \Sigma_n \frac{a_i}{10^i}$, and via the convergence rules in $\mathbb{Q}$ (to be discussed lated), the formal series $\Sigma_n \frac{a_i}{10^i}$ is *convergent* and *represents* the real number a.

b) The formal geometric series is $\boldsymbol{\sigma} :\overset{\text{def}}{=} \Sigma_n a^n = 1 + a + a^2 + \cdots + a^n + \ldots$

The above (formal) series $\boldsymbol{\sigma}$ is *convergent* for all rational/real/complex numbers $|a| < 1$, and *represents* the number $1/(a-1)$.

c) The harmonic series $\boldsymbol{\sigma} :\overset{\text{def}}{=} \sum_{n>0} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \ldots$ is a (formal) series which *does not represent* any rational/real/complex number.

d) Leibniz alternating series $\boldsymbol{\sigma} :\overset{\text{def}}{=} \sum_n \frac{(-1)^n}{n+1} = 1 - \frac{1}{2} + \frac{1}{3} - \ldots$ *represents* $\log(2)$.

e) The series $\boldsymbol{\sigma} :\overset{\text{def}}{=} \sum_n \frac{1}{n!} = 1 + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{n!} + \ldots$ *represents* the Euler number e.

f) Leibniz odd alternating series $\boldsymbol{\sigma} :\overset{\text{def}}{=} \Sigma_n \frac{(-1)^n}{2n+1} = 1 - \frac{1}{3} + \frac{1}{5} + \ldots$ *represents* $\frac{\pi}{4}$.

Proposition 5.16. *The set of series $\boldsymbol{\Sigma}(R)$ with coefficients from R endowed with the addition and multiplication of series is a commutative R-algebra. Precisely one has:*

(i) *The addition is associative, commutative, $0_{\boldsymbol{\Sigma}(R)} :\overset{\text{def}}{=} \sum_n 0_R$ is neutral element, and $-\Sigma_n a_n :\overset{\text{def}}{=} \Sigma_n(-a_n)$ is the inverse of $\Sigma_n a_n$ w.r.t. addition.*

(ii) *The multiplication is associative, commutative, and $1_{\boldsymbol{\Sigma}(R)} :\overset{\text{def}}{=} 1_R + \Sigma_{n>0} 0_R$ is neutral element. Moreover, $\Sigma_n a_n$ is invertible w.r.t. $\cdot$ iff $a_0 \in R$ is invertible w.r.t. $\cdot$ in R.*

(iii) *The multiplication is distributive w.r.t. addition.*

Proof. To (i): **Ex**... (easy direct checking).

To (ii): *Commutativity*: $(\Sigma_n a_n) \cdot (\Sigma_n b_n) :\overset{\text{def}}{=} \Sigma_n x_n$ with $x_n = \sum_{i+j=n} a_i \cdot b_j$, and $(\Sigma_n a_n) \cdot (\Sigma_n b_n) :\overset{\text{def}}{=} \Sigma_n y_n$ with $y_n = \sum_{j+i=n} b_j \cdot a_i$. Since R is commutative, $a_i \cdot b_j = b_j \cdot a_i$ for all i, j, hence $x_n = y_n$ for all $n \in \mathbb{N}$.

Associativity: One has $(\Sigma_n a_n) \cdot (\Sigma_n b_n) :\overset{\text{def}}{=} \Sigma_n x_n$ with $x_n = \sum_{i+j=n} a_i \cdot b_j$. Hence $\big((\Sigma_n a_n) \cdot (\Sigma_n b_n)\big) \cdot (\Sigma_n c_n) = (\Sigma_n x_n) \cdot (\Sigma_n c_n) = \Sigma_n y_n$, where $y_n :\overset{\text{def}}{=} \sum_{l+k=n} x_l \cdot c_k = (\sum_{i+j=l} a_i \cdot b_j) \cdot c_k = \sum_{i+j+k=n} a_i \cdot b_j \cdot c_k$. Deduce that the multiplication os series is associative (WHY).

Neutral element: $1_{\boldsymbol{\Sigma}(R)} = 1 + \Sigma_{n>0} 0_R$ is neutral element (**Ex**...)

Invertibility of $\Sigma_n a_n$: To $\Rightarrow$: Let $(\Sigma_n a'_n) \cdot (\Sigma_n a_n) = 1_{\boldsymbol{\Sigma}(R)}$. Then $a_0 \cdot a'_0 = 1_R$ (WHY), hence a_0 is invertible in R.

To $\Leftarrow$: Let $a'_0 \in R$ satisfy $a_0 \cdot a'_0 = 1_R$. We compute $(a'_n)_n$ such that $1_{\boldsymbol{\Sigma}(r)} = (\Sigma_n a_n) \cdot (\Sigma_n a'_n)$. Equivalently, one must have $a_0 \cdot a'_0 = 1_R$ and $\sum_{i+j=n} a_i \cdot a'_j = 0_R$ for all $n > 0$ (WHY). Computing a'_1: One has $n = 1$, hence must solve the equation $a_1 \cdot a'_0 + a_0 \cdot a'_1 = 0_R$ in the unknown a'_1. One has: $a_0 \cdot a'_1 = -a_1 \cdot a'_0$, hence recalling that $a'_0 \cdot a_0 = 1_R$, and multiplying by a'_0 get: $a'_1 = -a_1 \cdot (a'_0)^2$ (WHY). By induction, let $a'_1, \ldots, a'_{n-1}$ be computed s.t. $\Sigma_{i+j=l} a_i \cdot a'_j = 0_R$ for $0 \geqslant l < n$. We compute a'_n s.t. $\Sigma_{i+j=n} a_i \cdot a'_j = 0_R$. Equivalently, $a_0 \cdot a'_n = -(a_{n-1} \cdot a'_0 + \cdots + a_1 \cdot a'_{n-1})$ (WHY), implying that $a'_n :\overset{\text{def}}{=} -a'_0(a_n \cdot a'_0 + \cdots + a_1 \cdot a'_{n-1})$ (WHY).

To (iii): **Ex**... (direct verification using the distributivity of $\cdot$ w.r.t. $+$ in R). □

5.1.4. **Power Series and Polynomials over R.**

Definition 5.17. Let R be a commutative ring.

1) A symbol of the form $\Sigma_n a_n t^n$ is called a (formal) power series with coefficients $a_n \in R$ in the variable t. Let $R[\![t]\!]$ be the set of formal power series over R, and $0_{R[\![t]\!]} :\overset{\text{def}}{=} \sum_n 0t^n$.
2) $\Sigma_n a_n t^n \in R[\![t]\!]$ is called a polynomial if $a_n = 0_R$ for $n \gg 0$. Let $R[t] \subset R[\![t]\!]$ be the set of polynomials, and $0_{R[t]} :\overset{\text{def}}{=} \sum_n 0t^n = 0_{R[\![t]\!]}$. For $p(t) = \Sigma_n a_n t^n \in R[t]$, define the degree by:
$$\deg(0_{R[t]}) = -\infty, \quad \deg(p) = \max\{n \,|\, a_n \neq 0_R\} \text{ if } p(t) \neq 0_{R[t]}.$$

Examples 5.18. Let $R = \mathbb{Q}$, or more general $n1_R$ is invertible in R for all $n \in \mathbb{N}_{>0}$.

a) The geometric power series $f(t) = \Sigma_n t^n = 1 + t + \cdots + t^n + \ldots$
b) $\log(1+t) = \Sigma_n (-1)^n \frac{t^{n+1}}{n+1} = t - \frac{t^2}{2} + \frac{t^3}{3} - \cdots + (-1)^{n-1}\frac{t^n}{n} + \ldots$
c) $\exp(t) = \sum_n \frac{t^n}{n!} = 1 + \frac{t}{1!} + \frac{t^2}{2!} + \cdots + \frac{t^n}{n!} + \ldots$
d) $f(t) = 1 + t - t^2$ is a polynomial, with $\deg(f) = 2$.
e) The power series at a), b), c) are not polynomials.

Definition 5.19. Let R be an arbitrary commutative ring. Define in $R[\![t]\!]$ the addition $+$, multiplication $\cdot$, and multiplication by $a \in R$ as follows:

a) $(\Sigma_n a_n t^n) + (\Sigma_n b_n t^n) :\overset{\text{def}}{=} \Sigma_n c_n t^n$ where $c_n :\overset{\text{def}}{=} a_n + b_n$.
b) $(\Sigma_n a_n t^n) \cdot (\Sigma_n b_n t^n) :\overset{\text{def}}{=} \Sigma_n c_n t^n$, where $c_n :\overset{\text{def}}{=} \sum_{i+j=n} a_i \cdot b_j$.
c) $a \cdot (\Sigma_n a_n t^n) :\overset{\text{def}}{=} \Sigma_n a a_n t^n$.

Proposition 5.20. *Let R be a commutative ring. The following hold:*

1) *The set of formal power series $R[\![t]\!]$ with coefficients from R endowed with the addition and multiplication of series is a commutative R-algebra. Precisely one has:*
   (i) *The addition is associative, commutative, $0_{R[\![t]\!]}$ is neutral element, and $-\Sigma_n a_n t^n :\overset{\text{def}}{=} \Sigma_n (-a_n) t^n$ is the inverse of $\Sigma_n a_n t^n$ w.r.t. addition.*
   (ii) *The multiplication is associative, commutative, and $1_{R[\![t]\!]} :\overset{\text{def}}{=} 1_R + \Sigma_{n>0} 0_R t^n$ is neutral element. Moreover, $\Sigma_n a_n t^n$ is invertible w.r.t. $\cdot$ iff $a_0 \in R$ is invertible w.r.t. $\cdot$ in R.*
   (iii) *The multiplication is distributive w.r.t. addition.*
2) *The set of polynomials $R[t] \subset R[\![t]\!]$ is closed w.r.t. addition, multiplication, multiplication by $a \in R$, and $0_{R[\![t]\!]}, 1_{R[\![t]\!]} \in R[t]$, hence $R[t] \subset R[\![t]\!]$ is an R-subalgebra. Further one has:*
   a) $\deg(p+q) \leqslant \max\big(\deg(p), \deg(q)\big)$.
   b) $\deg(p \cdot q) \leqslant \deg(p) + \deg(q)$, *and equality holds if R is a domain, e.g., a field.*

Proof. To 1): **Ex** . . . (word-by-word the same as the proof of Proposition 5.16)

To 2): Let $p(t) = \Sigma_n a_n t^n, q(t) = \Sigma_n b_n t^n \in R[t]$ be given, $N_p :\overset{\text{def}}{=} \deg(p)$, $N_q :\overset{\text{def}}{=} \deg(g)$, hence $a_n = 0_R$ for $n > N_p$, and $b_n = 0_R$ for $n > N_q$ (WHY). First, if $p(t) + q(t) = h(t) = \Sigma_n c_n t^n$, then $c_n = a_n + b_n$. Hence if $n > N_p, N_q$, then $a_n = 0_R = b_n$, thus $c_n = 0_R$ (WHY). Conclude that $h(t) \in R[t]$ (WHY), and $\deg(h) \leqslant \max\big(\deg(p), \deg(q)\big)$. Second, $p(t) \cdot q(t) = h(t) = \Sigma_n c_n t^n$ with $c_n = \sum_{i+j=n} a_i \cdot b_j$. Hence if either $i > N_p$ or $j > N_q$, then $a_i \cdot b_j = 0_R$ (WHY). OTOH, if $n > N_p + N_q$, and $n = i + j$, then $i > N_p$ or

$j > N_q$ must hold (WHY). Hence for $n > N_p + N_q$ one has $c_n = 0_R$ (WHY). Conclude that $h(t) \in R[t]$, and $\deg(h) \leqslant N_p + N_q = deg(p) + \deg(q)$. Finally, if R is a domain, one has: Since $a_{N_p} \neq 0_R \neq b_{N_q}$, one has that $c_{N_p+N_q} = a_{N_p} \cdot a_{N_q} \neq 0_R$ (WHY), hence $\deg(p \cdot q) = \deg(p) + \deg(q)$. □

5.2. **Basic facts about totally ordered rings and field.**

Here we prove a few basic facts about *totally ordered domains* R, hence valid for all totally ordered fields, which generalize the known facts about $\mathbb{Z}$ and $\mathbb{Q}$. Recall that a domain is any commutative ring with cancellation, that means, satisfying the equivalent conditions:

(i) If $xy = 0_R$, then $x = 0_R$ or $y = 0_R$. (ii) If $xz = yz$ and $z \neq 0_R$, then $x = y$.

Proposition 5.21. *Let $R, +, \cdot$ be a domain, e.g. any field. The following hold:*

1) *Let $\leqslant$ be a total ordering of R compatible with addition and multiplication, and set $R_{\geqslant 0} := \{a \in R \,|\, x \geqslant 0\}$, $-R_{\geqslant 0} = \{-a \,|\, a \in R_{\geqslant 0}\}$. Then $\leqslant$ has cancellation, and furthermone has $R = -R_{\geqslant 0} \cup R_{\geqslant 0}$, $-R_{\geqslant 0} \cap R_{\geqslant 0} = \{0\}$ and $x \leqslant y$ iff $y - x \in R_{\geqslant 0}$.*
2) *Conversely, let $R_0 \subset R$ be a semiring, and setting $-R := \{-a \,|\, a \in R_0\}$, suppose that $R = -R_0 \cup R_0$ and $-R_0 \cap R_0 = \{0\}$. Then the relation $\leqslant$ on R defined by $x \leqslant y \overset{\text{def}}{\longleftrightarrow} y - x \in R_0$ is a total ordering of R such that $R_{\geqslant 0} = R_0$.*

In particular, in every totally ordered ring $R, +, \cdot, \leqslant$ with cancellation, the "sign rule" for products holds, i.e.: $x \cdot y > 0_R$ iff either $x, y > 0_R$ of $x, y < 0_R$. Hence $x^2 > 0_R$ for $x \neq 0_R$.

Proof. To 1): First we prove that $\leqslant$ has cancelation, i.e., to show that $\forall\, x, y, z \in R$ the following hold:

$$\text{(i) } x + z \leqslant y + z \Rightarrow x \leqslant y; \quad \text{(ii) } x \cdot z \leqslant y \cdot z \Rightarrow x \leqslant y, \text{ if } z > 0_R.$$

For $+$ one has: $x + z \leqslant y + z \overset{\text{why}}{\Rightarrow} (x + z) + (-z) \leqslant (y + z) + (-z) \overset{\text{why}}{\Rightarrow} x + \big(z + (-z)\big) \leqslant y + \big(z + (-z)\big) \overset{\text{why}}{\Rightarrow} x \leqslant y$. For $\cdot$, by contradiction, suppose that (ii) is wrong for some $x \cdot z \leqslant y \cdot y$ and $z > 0_R$, that is, there are $x, y, z \in R$, $z > 0_R$ such that the implication $x \cdot z \leqslant y \cdot z \Rightarrow x \leqslant y$ is wrong. Equivalently (WHY), $x \cdot z \leqslant y \cdot z$, $z > 0_R$, and $x > y$. OTOH, $x > y \Rightarrow u := x - y > 0_R$ (WHY). Hence multiplying by $z > 0_R$, one gets:

$$u > 0_R \overset{\text{why}}{\Rightarrow} u \cdot z > 0_R \overset{\text{why}}{\Rightarrow} (x - y) \cdot z > 0_R \overset{\text{why}}{\Rightarrow} x \cdot z - y \cdot z > 0_R \overset{\text{why}}{\Rightarrow} x \cdot z > y \cdot z, \quad \textbf{Contradiction!!!}$$

To 2): First prove that $\leqslant$ is an ordering: *reflexivity* $x \leqslant x$ is clear (WHY). For *antisymmetry*, if $x \leqslant y$ & $y \leqslant x$, then $x - y, y - x \in R_0$. Hence setting $z := x - y$, one has that $z, -z \in R_0$ (WHY), thus $z \in -R_0$, and finally $z \in -R_0 \cap R_0 = \{0_R\}$ (WHY), concluding that $x = y$ (WHY). Check that $\leqslant$ is a total ordering **Ex** . . . .

Finally, for the "sign rule," if $x < 0_R < y$, then $x \cdot y < 0_R$ (WHY). Second, $x, y > 0_R \overset{\text{why}}{\Rightarrow} x \cdot y > 0_R$; $x, y < 0_R \overset{\text{why}}{\Rightarrow} -x, -y > 0_R$, hence $(-x)(-y) > 0_R$. OTOH, $(-x)(-y) = (-1_R)^2 \cdot x \cdot y = x \cdot y$ (WHY). □

Remarks 5.22.

1) For $R = \mathbb{Z}$ and $\leqslant$ the natural ordering, one has $a \leqslant b \overset{\text{def}}{\longleftrightarrow} b = a + k$ with $k \in \mathbb{N}$ iff $b - a = k \in \mathbb{N}$ iff $b - a \geqslant 0_{\mathbb{Z}}$. Hence one recovers the definition of $\leqslant$ in $\mathbb{Z}$.

   For $R = \mathbb{Q}$ and $\leqslant$ the natural ordering, one has $x \leqslant y \overset{\text{def}}{\longleftrightarrow} y - x = \frac{a}{r}$ with $a, r \geqslant 0_Z$ iff $y - x = \frac{a}{r}$ with $\frac{a}{r} \geqslant 0_{\mathbb{Q}}$ (WHY). Hence one recovers the "usual" definition of $\leqslant$ in $\mathbb{Q}$.
2) Let $R, +, \cdot, \leqslant$ be a totally ordered domain. Since $1_R^2 = 1_R \neq 0_R$, one has $1_R > 0_R$ (WHY). Therefore, $n1_R > 0_R$ and $-n1_R = n(-1_R) < 0_R$ for all $n > 0$ (WHY). Hence one gets:

(∗) $\imath : \mathbb{Z} \to R$, $a \mapsto a1_R$ is injective and compatible with composition laws and $\leqslant$ (WHY).

And if $n1_R \in R^\times$, e.g. R is a field, for $\frac{a}{n} \in \mathbb{Q}$, define $\frac{a}{n}1_F :\overset{\text{def}}{=} (a1_F) \cdot (n1_F)^{-1}$. One gets:

(∗∗) $\imath : \mathbb{Q} \to F$, $\frac{a}{r} \mapsto \frac{a}{r}1_F$ is compatible with the composition laws and $\leqslant$ (WHY).

In the above situations, we denote the above embeddings by $\mathbb{Z} \hookrightarrow R$, respectively $\mathbb{Q} \hookrightarrow F$, and usually identify $a \in \mathbb{Z}$ with $a1_{\mathbb{Z}}$, respectively $x \in \mathbb{Q}$ with $x1_F$.

Definition/Remark 5.23 (The absolute value). Let $R, +, \cdot \leqslant$ be a totally ordered ring with cancellation. One defines

$$|\ |: R \to R_{\geqslant 0}, \quad |x| = \begin{cases} x & \text{if } x \geqslant 0_R \\ -x & \text{if } x \leqslant 0_R \end{cases}$$

and calls it the absolute value map (on R with respect to $\leqslant$).

The absolute value $|\ |: R \to R_{\geqslant 0}$ is *symmetric,* i.e., $|x-y| = |y-x|$, and $\forall\, x, y \in R$ satisfies:

(i) *Multiplicativity*: $|x \cdot y| = |x| \cdot |y|$.

(ii) *Subadditivity*: $\max(|x|, |y|) - \min(|x|, |y|) \leqslant |x+y|, |y-x| \leqslant |x| + |y|$.

Proof. First, $z \geqslant 0_F$ iff $-z \leqslant 0_F$, hence $|z| = |-z|$ (WHY); hence since $y-x = -(x-y)$, one has $|x-y| = |y-x|$ (WHY) for all $x, y \in F$. For the *multiplicativity,* and easy case-by-case consideration shows that $|x \cdot y| = |x| \cdot |y|$. For (ii) one has: Since $|-x| = |x|, |-y| = |y|, |x-y| = |y-x|, |x+y| = |-x-y|$, the value of the three terms of the inequalities are the same for any combination/choice of the signs $\pm x$, $\pm y$ (WHY). Hence w.l.o.g., we can suppose that $0_R \leqslant x \leqslant y$ (WHY). If so, one has $|x| = x, |y| = y, |y-x| = y-x, |x+y| = x+y = |x|+|y|$ (WHY), and the inequalities are obvious (WHY). □

Sections 5.3 & 5.4 are optional (Study them if you are a math major!)

5.3. The group attached to a commutative monoid.

Definition 5.24. Let $X, *$ be a set endowed with a composition law. One says that $*$ has left cancellation, or the left cancellation property, if for all $x, y, z \in X$ one has: $z*x = z*y \Rightarrow x = y$. Define correspondingly the right cancellation, and notice that if $*$ is commutative, then left/right cancellations are equivalent (WHY).

Example 5.25. The following hold:

- $\mathbb{N}, +$ and $\mathbb{N}_{>0}, \cdot$ have cancellation (WHY).
- Which among the composition laws $\cup$, $\cap$, Δ on $X := \mathcal{P}(A)$ have cancellation?
- Is there cancellation in the monoid $\mathrm{Maps}(X), \circ$?

Proposition 5.26. *Let $M, *$ be a commutative monoid. On the set $M \times M$ consider the relation $(a,b) \sim (a',b') \overset{\text{def}}{\longleftrightarrow} \exists\, x \in M$ s.t. $a*b'*x = a'*b*x$. Then the following hold:*

1) *The relation $\sim$ is an equivalence relation on the set $M \times M$. For $(a,b) \in M \times M$, let $\overline{(a,b)}$ be its equivalence class, and set $G \overset{\text{def}}{:=} M \times M/\sim$ be the set of equivalence classes.*
2) *Define on G the composition law: $\overline{(a,b)} * \overline{(c,d)} \overset{\text{def}}{:=} \overline{(a*c, b*d)}$. Then $*$ is well defined, and $G, *$ is a group, with $e_G := \overline{(e_M, e_M)} = \overline{(a,a)}$, and $\overline{(a,b)}^{-1} = \overline{(b,a)}$ for all $a, b \in M$.*
3) *Moreover, suppose that $M, *$ has cancellation. Then $(a,b) \sim (a',b')$ iff $a*b' = a'*b$, and the map $\imath : M \to G$ by $a \mapsto \overline{(a,e)}$ is injective, and satisfies $\imath(a*b) = \imath(a) * \imath(b)$.*

Proof. **Ex** . . . (direct checking) □

Example 5.27. The additive group of integer numbers $\mathbb{Z},+$

Let $M,*$ be $\mathbb{N},+$. Then one has $(k,l)\sim(k',l')\overset{\text{def}}{\longleftrightarrow}k+l'=k'+l$. Therefore, the equivalence relation $\sim$ is the previously defined equivalence relation on $\mathcal{Z}:=\mathbb{N}\times\mathbb{N}$, and the above abstract construction for $M,*$ delivers the additive group $\mathbb{Z},+$ of the integer numbers with the usual addition of such numbers.

Example 5.28. The multiplicative group of positive rational numbers $\mathbb{Q}_{>0}$

Let $M,*$ be $\mathbb{N}_{>0}$ endowed with the multiplication $\cdot$. Then $(n,m)\sim(n',m')$ iff $n\cdot m'=n'\cdot m$ (WHY). In particular, this is the previously equivalence relation on $\mathcal{N}\subset\mathcal{Z}$ used to define the rational numbers. The resulting group attached to $M,*$ is the group of positive rational numbers w.r.t. multiplication (WHY).

5.4. The ring/field attached to a semiring/semifield.

Definition 5.29.

1) A commutative semiring is a set $\mathcal{R}$ endowed with two composition laws: addition $+$ and multiplication $\cdot$ such that $\mathcal{R},+$ and $\mathcal{R},\cdot$ are monoids, and $\cdot$ is distributive w.r.t. $+$. One denotes the neutral elements of $+$ and $\cdot$ by $0_{\mathcal{R}}$, respectively $1_{\mathcal{R}}$, and called them the zero element, respectively the unit element of $\mathcal{R}$.
2) A semifield is a commutative semiring $\mathcal{F},+,\cdot$ such that every $x\in\mathcal{F}$, $x\neq 0_{\mathcal{F}}$ is invertible w.r.t. the multiplication $\cdot$, i.e., $\mathcal{F}^{\times}:=\mathcal{F}\setminus\{0_{\mathcal{F}}\}$ endowed with $\cdot$ is a commutative group.

Example 5.30. On has the following:

a) $\mathbb{N},+,\cdot$ is a commutative semiring (WHY).
b) $\mathbb{Q}_{\geqslant 0},+,\cdot$ is a semifield (WHY).

Proposition 5.31. *Let $\mathcal{R},+,\cdot$ be a commutative semiring such that $+$ has cancellation, and let $R,\oplus$ be the monoid attached to $\mathcal{R},+$. Further, denote the equivalence class $\overline{(a,b)}$ by $(a\text{-}b):\overset{\text{def}}{=}\overline{(a,b)}$ for $a,b\in\mathcal{R}$, and set $1_R:=(1\text{-}0_{\mathcal{R}})$. Define on R a multiplication $\odot$ by the rule:*

$$(a\text{-}b)\odot(c\text{-}d)\ :\overset{\text{def}}{=}\ ((a\cdot c+b\cdot d)\text{-}(a\cdot d+b\cdot c))\,.$$

Then the multiplication $\odot$ is well defined, and the following hold:

1) *Then $R,\oplus,\odot$ is a commutative ring with 1_R as above, and $\imath:\mathcal{R}\to R$ by $\imath(a)=(a\text{-}0_{\mathcal{R}})$ is injective and satisfies: $\imath(a+b)=\imath(a)\oplus\imath(b)$, $\imath(a\cdot b)=\imath(a)\odot\imath(b)$,*
2) *Moreover, if $\mathcal{F},+,\cdot$ is a semifield, then the corresponding $F,\oplus,\odot$ is a field.*

Proof. **Ex** (the proof is virtually identical with the one constructing $\mathbb{Z},+,\cdot$ from the semiring $\mathbb{N},+,\cdot$, etc.) □

Terminology/Convention. In the above context, $R,\oplus,\odot$ and $F,\oplus,\odot$ are called the ring, respectively field, attached to $\mathcal{R}$, respectively $\mathcal{F}$. Via the embedding $\imath:\mathcal{R}\to R$, one identifies $a\in\mathcal{R}$ with $\imath(a)\in R$, thus views $\mathcal{R}$ as a subset of R. One gets identifications:

$$0_{\mathcal{R}}=(0_{\mathcal{R}}\text{-}0_{\mathcal{R}})=0_R,\quad 1_{\mathcal{R}}=(1_{\mathcal{R}}\text{-}0_{\mathcal{R}})\,,\quad a=\imath(a)=(a\text{-}0_{\mathcal{R}})$$

Notice that under these identifications one has: $\imath(a)-\imath(b)=(a\text{-}b)=a-b$ for all $a,b\in\mathcal{R}$ (WHY).

Example 5.32. On has the following:

a) The ring attached to the semi-ring $\mathbb{N}, +, \cdot$ is $\mathbb{Z}, +, \cdot$ (WHY).

b) The field attached to the division semi-field $\mathbb{Q}_{\geqslant 0}, +, \cdot$ is $\mathbb{Q}, +, \cdot$ (WHY).

6. More about Sequences

6.1. **Generalities about sequences.** We first introduce a notation to be used throughout the remaining part of these notes:

"... for $n \gg 0$" means "there is $N \in \mathbb{N}$ such that for all $n \geqslant N$ one has ..."

Example 6.1. The two assertions in quotations marks at a), b), c) below are identical (WHY):

a) "*there is* $N \in \mathbb{N}$ *such that for all* $n \geqslant N$ *one has* $n > a$" "$n > a$ *for* $n \gg 0$"

b) "*there is* $N \in \mathbb{N}$ *s.t. for* $n \geqslant N$ *one has* $|a_n - a| < \epsilon$" "$|a_n - a| < \epsilon$ *for* $n \gg 0$"

c) "*there is* $N \in \mathbb{N}$ *s.t.* $\forall\, m, n \geqslant N$ *one has* $|a_n - a_m| < \epsilon$" "$|a_n - a_m| < \epsilon$ *for* $m, n \gg 0$"

Definition 6.2.

1) Let X be an arbitrary set. A sequence with value in X is any map $\boldsymbol{x} : \mathbb{N} \to X$. The elements $x_n := \boldsymbol{x}(n)$ are called the terms of the sequence. Notation. $(x_n)_n \overset{\text{not}}{=} \boldsymbol{x}$

Notation. $\mathcal{S}(X) := \{\boldsymbol{x} = (x_n)_n \,|\, \boldsymbol{x} : X \to \mathbb{N}\}$ is the set of sequences with values in X.

2) Let $\boldsymbol{x} = (x_n)_n \in \mathcal{S}(X)$ be given. A subsequence of $(x_n)_n$ is any sequence $(x_{n_k})_k$ defined by the composition of a strictly increasing map $\boldsymbol{n} : \mathbb{N} \to \mathbb{N}$, $\boldsymbol{n}(k) =: n_k$ and $\boldsymbol{x} : \mathbb{N} \to X$. In other words, $(x_{n_k})_k$ is given by $x_{n_k} := \boldsymbol{x}(n_k) := \boldsymbol{x}\Big(\boldsymbol{n}(k)\Big)$ for all $k \in \mathbb{N}$.

3) Two sequences $(x_n)_n, (y_n)_n \in \mathcal{S}(X)$ are almost equal, if $x_n = y_n$ for $n \gg 0$.
And $(x_n)_n$ is almost constant, if $\exists\, x \in X$ such that $x_n = x$ for $n \gg 0$..

4) A sequence $(x_n)_n$ is called almost periodic, if there is $k \in \mathbb{N}$, called (almost) period, such that $x_{n+k} = x_n$ (for $n \gg 0$).

Example 6.3. Here are a few examples of types of sequences:

a) (Almost) periodic sequences:
- The alternating sequence $(x_n)_n$, $x_n = (-1)^n$ is the typical periodic sequence (WHY).
- $(x_n)_n$ with $x_n = \Big(n^{\text{th}}$ decimal digit of $\frac{1}{3}\Big)$ is almost periodic. What is the period?
  Same question for $(x_n)_n$ with $x_n = \Big(n^{\text{th}}$ decimal digit of $\frac{25}{12}\Big)$.
- $(x_n)_n$ with $x_n = \Big($remainder of division of n by a fixed $m > 0\Big)$.

b) $(x_n)_n$, $x_n = \Big($number of prime factors of $n\Big)$ with values in $\mathbb{N}$ is a quite *random sequence.*

c) Recurrence sequences:
- $(x_n)_n$ with $x_0 = 10$, $x_{n+1} = x_n + 2$. What is x_n ?
- a, b fixed, x_0, x_1 given, and $x_{n+2} = bx_{n+1} + ax_n$. What is x_n ?

Famous sequences:

- The e-sequence: $(x_n)_n$ with $x_n = (1 + \frac{1}{n})^n$, $n > 0$.

- The Euler sequence: $(E_n)_n$ with $E_0 = 1$, $E_{n+1} = E_n + \frac{1}{(n+1)!}$. What is E_n ?
- The Fibonacci sequence $(F_n)_n$ has values in $\mathbb{N}$, being defined inductively as follows: $F_0 = 0, F_1 = 1$, and inductively $F_{n+1} = F_n + F_{n-1}$ for $n > 0$.
- The Leibniz sequence $(a_n)_n$, defined inductively by $a_0 = 1$, $a_{n+1} = a_n + \frac{(-1)^n}{2n+1}$.

Definition 6.4. Let $\leqslant$ be a (partial) ordering of X, and $\boldsymbol{x} = (x_n)_n \in \mathcal{S}(X)$ be given.

1) $(x_n)_n$ is called (strictly) increasing, if the map $\boldsymbol{x} : \mathbb{N} \to X$ is (strictly) increasing, that is, $\forall\, n \in \mathbb{N}$ one has: $x_n \leqslant x_{n+1}$ (respectively $x_n < x_{n+1}$).
   Define correspondingly (strictly) decreasing.
2) $(x_n)_n$ is (strictly) monotone, if it is either (strictly) increasing or (strictly) decreasing.

Definition/Remark 6.5. Let $\leqslant$ be a (partial) ordering of X, and $\boldsymbol{x} = (x_n)_n \in \mathcal{S}(X)$ be given, and $\boldsymbol{x}(\mathbb{N}) = \{x_n \,|\, n \in \mathbb{N}\}$ be its set of values. **Warning:** Do not confuse $\boldsymbol{x}(\mathbb{N})$ with $(x_n)_n$.

1) $(x_n)_n$ is bounded (below) [above] if the set of values $\boldsymbol{x}(\mathbb{N})$ is bounded (below) [above] in X.
2) If $(x_n)_n$ if bounded (below) [above], so are all the subsequences $(x_{n_k})_k$ of $(x_n)_n$.

Notation. Let $\mathcal{S}_{\mathrm{b}}(X)$ be set of all bounded sequences with values in X.

Ex. Which of the sequences in Example 6.3 are (strictly) monotone, bounded above/below?

Construction 6.6 (min/max construction). Let $X, \leqslant$ be totally ordered, $(x_n)_n \in \mathcal{S}(X)$.
The max construction: One of the following two cases holds:

Case 1. For every $n \in \mathbb{N}$ one has: $\max\{x_{n'} \,|\, n' \geqslant n\}$ does not exist.
If so, set $n_0 = 0$ and define $(n_k)_k$ inductively by $n_{k+1} := \min\{n' \in \mathbb{N} \,|\, n_k < n', x_{n_k} < x_{n'}\}$.
Then $(x_{n_k})_k$ is a strictly *increasing subsequence* of $(x_n)_n$ (WHY).

- Hence setting $x'_n = x_{n_k}$ for $n_k \leqslant n < n_{k+1}$ for $k \in \mathbb{N}$, one has:
  (i) $(x'_n)_n$ is increasing; (ii) $x_n \leqslant x'_n \;\forall\, n \in \mathbb{N}$; (iii) $x_{n_k} = x'_{n_k} \;\forall\, k \in \mathbb{N}$.

Case 2. For every $n \in \mathbb{N}$ one has: $y_n := \max\{x_{n'} \,|\, n' \geqslant n\}$ exists.
Set $n_0 = \min\{n \in \mathbb{N} \,|\, y_n = y_0\}$ and set inductively $n_{k+1} := \min\{n' \in \mathbb{N} \,|\, n_k < n', x_{n'} = y_{n'}\}$.
Then $(x_{n_k})_k$ is a *decreasing subsequence* of $(x_n)_n$ (WHY), and one of the following cases hold:

(i) $(x_{n_k})_k$ is almost constant, i.e., $\exists\, x \in X$ s.t. $x_{n_k} = x$ for $k \gg 0$ (WHY).
(ii) The sequence $(x_{n_k})_k$ is not almost constant. Then $\forall\, k \in \mathbb{N}\; \exists\, k' > k$ s.t. $x_{n_{k'}} < x_{n_k}$ (WHY).
Define inductively $\boldsymbol{n} = (n_l)_l$ $n_0 = n_0$ and $n_{l+1} = \min\{n_{k'} \in \mathbb{N} \,|\, l < k', x_{n_{k'}} < x_{n_l}\}$.
Then $(x_{n_l})_l$ is a *strictly decreasing* subsequence of $(x_{n_k})_k$, hence of $(x_n)_n$ (WHY).

- Hence setting $x'_n = x_{n_l}$ for $n_l \leqslant n < n_{l+1}$ for $l \in \mathbb{N}$, one has:
  (i) $(x'_n)_n$ is decreasing; (ii) $x_n \leqslant x'_n \;\forall\, n \in \mathbb{N}$; (iii) $x_{n_l} = x'_{n_l} \;\forall\, l \in \mathbb{N}$.

Ex. Perform the min/max construction by reversing the roles of min and max. The result?
Ex. Perform the min/max construction on the sequences in Example 6.3.

Fact 6.7. Let $(x_n)_n \in \mathcal{S}(X)$ with $X, \leqslant$ totally ordered be given. Then the exist monotone sequences $(x'_n)_n$, $(x''_n)_n$ having subsequences $(x'_{n_k})_k$, $(x''_{n_l})_l$ satisfying:

(i) $x''_n \leqslant x_n \leqslant x'_n \;\forall\, n \in \mathbb{N}$; (ii) $x''_{n_l} = x_{n_l}$ and $x'_{n_k} = x_{n_k} \;\forall\, l, k \in \mathbb{N}$.

Proof. **Ex** (**Hint**: The max construction gives $(x'_n)_n$, the min construction gives $(x''_n)_n$, etc ...). □

6.2. **Convergent sequences / Cauchy sequences.**

We next discuss basics about convergent sequences, respectively Cauchy sequences $(a_n)_n$ with values in a totally ordered field $F, +, \cdot, \leqslant$, one of the main examples being $\mathbb{Q}, +, \cdot, \leqslant$.

Definition 6.8. Let $F, +, \cdot, \leqslant$ be a totally ordered field, $|\ |: F \to F$ be the abs value map.

1) A sequence $(a_n)_n \in \mathcal{S}(F)$ is called convergent, if there is some $a \in F$ satisfying:
$\forall\, \epsilon > 0_F\ \exists\, N \in \mathbb{N}$ s.t. $\forall\, n > N$ one has: $|a_n - a| < \epsilon$. (Equiv: $|a_n - a| < \epsilon$ for $n \gg 0$.)

Notation. $a_n \to a$, or $\lim\limits_{n\to\infty} x_n = a$. [read "$a_n$ tends to a" or "$(a_n)_n$ has limit a"]

Notation. Let $\mathcal{S}_{\rm c}(F)$ be set of all convergent sequences with values in F.

2) A sequence $(a_n)_n \in \mathcal{S}(F)$ is called Cauchy sequence, if it satisfies:
$\forall\, \epsilon > 0_F\ \exists\, N = N_\epsilon \in \mathbb{N}$ s.t. $\forall\, m, n > N$ one has: $|a_n - a_m| < \epsilon$. (Equiv: $|a_n - a_m| < \epsilon$ for $m, n \gg 0$.)

Notation. Let $\mathcal{S}_{\rm C}(F)$ be set of all Cauchy sequences with values in F.

3) A sequence $(a_n)_n \in \mathcal{S}(F)$ is called bounded away from 0_F, if there exists $\epsilon_0 > 0_F$ and $N \in \mathbb{N}$ such that for $N > N$ one has $|a_n| > \epsilon$. (Equiv: $|a_n| > \epsilon$ for $n \gg 0$).

Ex. Let $(a_n)_n \in \mathcal{S}(F)$ be a sequence, and let $\prec$ denote $\leqslant, <$ in no particular order, respectively $\succ$ denote $\geqslant, >$ in no particular order. Prove the following:

1) $a_n \to a$ iff $\forall\, \epsilon > 0_F\ \exists\, N \in \mathbb{N}$ such that $\forall\, n \succ N$ one has: $|a_n - a| \prec \epsilon$.
2) $(a_n)_n$ is Cauchy iff $\forall\, \epsilon > 0_F\ \exists\, N \in \mathbb{N}$ such that $\forall\, n, m \succ N$ one has: $|a_n - a_m| \prec \epsilon$.
3) $(a_n)_n$ is bounded away from 0_F if $\exists\, \epsilon > 0_F$ and $\exists\, N \in \mathbb{N}$ s.t. $\forall\, n \succ N$ one has $|a_n| \succ \epsilon$.

In particular, in the definition of convergence and/or Cauchy and/or bounded away from 0_F, the conditions $<$ and $>$ can be replaced by $\leqslant$ and/or $\geqslant$, **except for the condition** $\epsilon > 0_F$.

Remark 6.9. Recall that in the above notation, $\mathcal{S}(F) = \mathrm{Maps}(\mathbb{N}, F)$ is an F-algebra w.r.t. the usual addition and multiplication of maps, i.e., of sequences, defined by

$$(a_n)_n + (b_n)_n :\overset{\text{def}}{=} (a_n + b_n)_n, \qquad (a_n)_n \cdot (b_n)_n :\overset{\text{def}}{=} (a_n \cdot b_n)_n, \qquad a \cdot (a_n)_n :\overset{\text{def}}{=} (a \cdot a_n)_n\ \forall\, a \in F,$$

and having the constant 0_F-sequnce $0_{\mathcal{S}(F)}$ as the neutral element for the addition, and the constant 1_F-sequnce as neutral element $1_{\mathcal{S}(F)}$ for the multiplication.

Proposition 6.10. *In the above notation, the following hold:*

1) *If $(a_n)_n \in \mathcal{S}(F)$ is convergent, there is $a \in F$ **unique** s.t. $a_n \to a$. Further, one has:*
   a) *Every subsequence $(a_{n_k})_k$ of $(a_n)_n$ is convergent, and $a_{n_k} \to a$.*
   b) *If $(b_n)_n \in \mathcal{S}(F)$ is almost equal to $(a_n)_n$, then $b_n \to a$.*
2) *If $(a_n)_n \in \mathcal{S}(F)$ is convergent, then $(a_n)_n$ is Cauchy. Further, if a Cauchy sequence $(a_n)_n \in \mathcal{S}(F)$ has a convergent subsequence $(a_{n_k})_k$, say $a_{n_k} \to a$, then $a_n \to a$.*
3) *Let $(a_n)_n$ be a Cauchy sequence. Then $(a_n)_n$ is bounded, and further one has:*
   a) *Every subsequence $(a_{n_k})_k$ of $(a_n)_n$ is a Cauchy sequence.*
   b) *If $(a_n)_n$ and $(b_n)_n$ are almost equal, then $(b_n)_n$ is Cauchy.*
4) *Let $(a_n)_n$ be such that $a_n \neq 0_F$ for all $n \in \mathbb{N}$. The following hold:*
   a) *$(a_n)_n$ is bounded and bounded away from 0_F iff $\left(\frac{1}{a_n}\right)_n$ is so.*

b) *If $(a_n)_n$ is Cauchy and $a_n \not\to 0_F$, There is $\epsilon > 0_F$ and $N \in \mathbb{N}$ such that either $\epsilon \leqslant a_n$ or $a_n \leqslant -\epsilon$ for $n \geqslant N$. Further, $\left(\frac{1}{a_n}\right)_n$ is Cauchy and $\frac{1}{a_n} \not\to 0_F$*

Proof. To 1): By contradiction, suppose that $a_n \to a$ and $a_n \to b$ with $a \neq b$. Then $b-a \neq 0_F$, and therefore, $\epsilon := \frac{1}{2}|b-a| > 0_F$. Since $a_n \to a$ and $y_n \to b$, there are N', N'' be such that $\forall\, n' > N'$ and $\forall\, n'' > N''$ one has: $|a_{n'} - a| < \epsilon$, $|a_{n''} - b| < \epsilon$. Hence for $n > \max(N', N'')$ one has:

$|b-a| = |b + (a_n - a_n) - a| = |(a_n - a) - (a_n - b)| \leqslant |a_n - a| + |a_n - b| < 2\epsilon = |b-a|$, **contradiction!**

To 1a): Let $\epsilon > 0_F$ be given. Since $(a_n)_n$ is convergent, $\exists N \in \mathbb{N}$ s.t. $\forall\, n > N$ one has $|a_n - a| < \epsilon$. OTOH, for all $k \in \mathbb{N}$ one has $n_k \geqslant k$ (WHY), and therefore, for $k > N$ one has $|a_{n_k} - a| < \epsilon$. Thus $a_{n_k} \to a$.

To 1b): Since $(a_n)_n$ and $(b_n)_n$ are almost equal, $\exists, N_0 \in \mathbb{N}$ such that for $n > N_0$ one has $a_n = b_n$. Hence for $n > N_0$ one has $|b_n - a| = |a_n - a|$, etc.

To 2): Let $(a_n)_n$ satisfy $a_n \to a$. We show that $(a_n)_n$ is Cauchy. Indeed, given $\epsilon > 0_F$, set $\epsilon' := \frac{1}{2}\epsilon$. Then $\epsilon' > 0_F$ (WHY), hence $\exists\, N \in \mathbb{N}$ such that $\forall\, n \geqslant N$ one has $|a_n - a| < \epsilon'$ (WHY). Thus for $n, m > N$ one gets:

$|a_n - a_m| = |a_n - a_N + a_N - a_m| \leqslant |a_n - a_N| + |a_N - a_m| < \epsilon' + \epsilon' = \epsilon$, hence $(a_n)_n$ is Cauchy.

Next let $(a_{n_k})_k$ be a convergent subsequence, say $a_{n_k} \to a$. We prove that $x_n \to a$. Namely, for $\epsilon > 0_F$, set $\epsilon' := \frac{1}{2}\epsilon$. Then $\epsilon' > 0_F$ (WHY), hence $\exists\, N' \in \mathbb{N}$ such that $\forall\, m, n \geqslant N'$ one has $|a_n - a_m| < \epsilon'$ (WHY). Further, there is $N'' \in \mathbb{N}$ s.t. $\forall\, k > N''$ one has: $|a_{n_k} - a| < \epsilon'$. Thus setting $N = \max(N', N'')$, for $n, k > N$ one has $n, n_k > N'$ and $k > N''$, and therefore one gets:

$|a_n - a| = |a_n - a_{n_k} + a_{n_k} - a| \leqslant |a_n - a_{n_k}| + |a_{n_k} - a| < 2\epsilon' = \epsilon$, implying that $a_n \to a$.

To 3): We prove that every Cauchy sequence $(a_n)_n$ is bounded. Choose any $\epsilon_0 > 0_F$. Since $(a_n)_n$ is Cauchy, $\exists\, N = N_{\epsilon_0}$ such that $\forall\, n, m \geqslant N$ one has $|a_n - a_m| > \epsilon_0$ (WHY). Since $X_N := \{|a_i| \,|\, i \leqslant N\} \subset F$ is finite, $\epsilon_N = \max(X_N) \geqslant 0_F$ exists. Then $\forall\, n \in N$ one has: $|a_n| = |a_n - a_N + a_N| \leqslant |a_n - a_N| + |a_N| \leqslant \epsilon_0 + \epsilon_N$. Therefore, for all $n \in \mathbb{N}$ one has: $-(\epsilon_0 + \epsilon_N) < a_n < \epsilon_0 + \epsilon_N$ (WHY), thus $(a_n)_n$ is bounded.

To 3a) & 3b): **Ex** . . . (proceed as in the proof of 1a) & 1b) above).

To 4a): "$\Rightarrow$": $(a_n)_n$ bounded & bounded away from 0_F $\Rightarrow$ $\left(\frac{1}{a_n}\right)_n$ bounded an bounded away from 0_F.

Indeed: (i) Since $(a_n)_n$ is bounden, $\exists c > 0_F$ s.t. $\forall\, n \in \mathbb{N}$ one has $|a_n| < c$ (WHY). (ii) Since $(a_n)_n$ bounden away from 0_F, $\exists c_0 > 0_F$ s.t. $\forall\, n \in \mathbb{N}$ one has $1/|a_n| > c_0$ (WHY). Hence for all $n \in \mathbb{N}$ one has: (i)$'$ $\left|\frac{1}{a_n}\right| > 1/c$. (ii)$'$ $|a_n| < 1/c_0$ (WHY). Conclude that $\left(\frac{1}{a_n}\right)_n$ is bounded and bounded away from 0_F (WHY).

"$\Leftarrow$" **Ex** . . . .

To 4b): First, since $a_n \not\to 0_F$, there is $\epsilon' > 0_F$ s.t. for every $N > 0$ there is $m \geqslant N$ s.t. $|a_m| = |a_m - 0_F| > \epsilon'$ (WHY). Second, since $(a_n)_n$ is Cauchy, for $\epsilon := \frac{1}{2}\epsilon'$ $\exists\, N \in \mathbb{N}$ such that $|a_n - a_m| < \epsilon$ for all $m, n > N$, or equivalently, $-\epsilon < x_n - x_m < \epsilon$. Let $m > N$ be fixed such that $|a_m| > \epsilon'$, hence either (i) $a_m < -\epsilon'$, or (ii) $\epsilon' < a_m$. In case (i), one has: $a_n = (a_n - a_m) + a_m < \epsilon - \epsilon' = -\epsilon$ for all $n \geqslant N$ (WHY). In case (ii), one has: $a_n = a_n - a_m + a_m > -\epsilon + \epsilon' = \epsilon$ for all $n \geqslant N$. (WHY). Finally we prove that $\left(\frac{1}{a_n}\right)_n$ is Cauchy. Let $\epsilon > 0_F$ be given, and set $\epsilon' := \epsilon \cdot \epsilon_1^2 > 0_F$. Since $(a_n)_n$ is Cauchy, there is $N \in \mathbb{N}$ such that $\forall m, n > N$ one has: $|a_m - a_n| < \epsilon'$. With this choices one has: $\left|\frac{1}{a_n} - \frac{1}{a_m}\right| = \left|\frac{a_m - a_n}{a_n a_m}\right| = |a_m - a_n|/|a_n||a_m| < \epsilon'/\epsilon_1^2 = \epsilon$. Hence we conclude that $\left(\frac{1}{a_n}\right)_n$ is a Cauchy sequence. □

Proposition 6.11. *In the above notation, let $\mathcal{S}_{\mathrm{c}}(F) \subset \mathcal{S}_{\mathrm{C}}(F) \subset \mathcal{S}(F)$ be the subsets of convergent, respectively Cauchy sequences in the F-algebra of all the F-valued sequences $\mathcal{S}(F)$. For sequences $(a_n)_n \in \mathcal{S}(F)$, the following hold: following hold:*

1) *$(a_n)_n$ is convergent / Cauchy iff $(aa_n)_n$ is convergent / Cauchy for some (all) $a \neq 0_F$.*
2) *Let $a_n \to a$, $b_n \to b$. Then $a_n - b_n \to a - b$; $a_n \cdot b_n \to a \cdot b$; $\frac{1}{a_n} \to \frac{1}{a}$ if $a_n, a \neq 0_F$.*
3) *Let $(a_n)_n, (b_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$. Then $(a_n - b_n)_n$, $(a_n \cdot b_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$.*
4) *Let $(a_n)_n, (b_n)_n \in \mathcal{S}_{\mathrm{b}}(F)$. Then $(a_n - b_n)_n$, $(a_n \cdot b_n)_n \in \mathcal{S}_{\mathrm{b}}(F)$.*

In particular, $\mathcal{S}_{\mathrm{c}}(F) \subset \mathcal{S}_{\mathrm{C}}(F) \subset \mathcal{S}_{\mathrm{b}}(F) \subset \mathcal{S}(R)$ are F-subalgebras of $\mathcal{S}(R)$. Moreover, $(a_n)_n \in \mathcal{S}_\bullet(F)$ is invertible in $\mathcal{S}_\bullet(F)$ iff $(a_n)_n$ is bounded away from zero.

Proof. To 1): **Ex** . . .

To 2): Given: $a_n \to a$, $b_n \to b$. To prove: $(a_n - b_n)_n \to a - b$; $(a_n \cdot b_n)_n \to a \cdot b$; $\frac{1}{a_n} \to \frac{1}{a}$ if $a_n, a \neq 0_F$.

• Proof of $a_n - b_n \to a - b$. Let $\epsilon > 0_F$ be given. Set $\epsilon' := \frac{1}{2}\epsilon$, and N', N'' be such that for all $n' > N'$, $n'' > N''$ one has: $|a_{n'} - a| < \epsilon'$ and $b_{n''} - b| < \epsilon'$. Hence setting $N = \max(N', N'')$ for all $n > N$ one has:

$$|(a_n - b_n) - (a - b)| \leqslant |(a_n - a) - (b_n - b)| \leqslant |a_n - a| + |b_n - b| < \epsilon' + \epsilon' = \epsilon.$$

• Proof of $a_n \cdot b_n \to a \cdot b$. Let $\epsilon > 0_F$ be given, and $c > 0_F$ be such that $|b_n| \leqslant c \; \forall\, n \in \mathbb{N}$; **Note** such c exist (WHY). Let $\epsilon' = \epsilon/(c + |a|) > 0$, and N', N'' be such that for all $n' > N'$, $n'' > N''$ one has: $|a_{n'} - a| < \epsilon'$ and $|b_{n''} - b| < \epsilon'$. Hence setting $N = \max(N', N'')$ for all $n > N$ one has:

$$|(a_n \cdot b_n) - (a \cdot b)| \leqslant |a_n - a \cdot b_n + a \cdot b_n - a \cdot b| \leqslant |a_n - a| \cdot c + |a| \cdot |b_n - b| < \epsilon' \cdot c + |a| \cdot \epsilon' = \epsilon'(c + |a|) = \epsilon.$$

• Proof of $\frac{1}{a_n} \to \frac{1}{a}$. Since $a \neq 0_F$, one has $|a| > 0_F$ (WHY), hence for $c\epsilon' := \frac{1}{2}|a| > 0_F$, there is N such that $\forall\, n > N$ one has $|a_n - a| < \epsilon' = \frac{1}{2}|a|$. Hence since $|a| > \frac{1}{2}|a| = \epsilon' \geqslant |a_n - a|$, one has $|a_n| = |(a_n - a) + a| \geqslant |a| - |a_n - a| \geqslant \frac{1}{2}|a|$. Now let $\epsilon > 0_F$ be given. Set $\epsilon'' = \frac{1}{2}|a|^2\epsilon > 0_F$. Since $a_n \to a$, there is N such that $\forall\, n \in \mathbb{N}$ one has: $|a_n - a| < \epsilon''$. Hence for all $n > N$ one has:

$$|\tfrac{1}{a_n} - \tfrac{1}{a}| \overset{\text{why}}{=} |\tfrac{a - a_n}{a a_n}| \overset{\text{why}}{=} |a_n - a|/(|a_n||a|) \leqslant \epsilon''/(\tfrac{1}{2}|a||a|) = \epsilon.$$

To 3): The inclusion $\mathcal{S}_{\mathrm{c}}(F) \subset \mathcal{S}_{\mathrm{C}}(F) \subset \mathcal{S}_{\mathrm{b}}(F)$ follows from Proposition 6.10, 2), 3). Finally, from the assertions 1), 2), 3) above, it follows that $\mathcal{S}_{\mathrm{c}}(F) \subset \mathcal{S}_{\mathrm{C}}(F) \subset \mathcal{S}_{\mathrm{b}}(F)$ are F-subalgebras of $\mathcal{S}(F)$ (WHY). □

6.3. **Convergence of series / power series.**

We discuss (briefly) the convergence of series (parallel to the convergence of sequences).

Definition 6.12. Let F be a totally ordered field, and consider series $\Sigma_n a_n \in \sum(F)$.

1) The sequence of partial sums $(s_n)_n$ of $\Sigma_n a_n$ is defined by $s_n :\overset{\text{def}}{=} \sum_{i \leqslant n} a_i = a_0 + \cdots + a_n$.
2) $\Sigma_n a_n$ is called convergent, if $(s_n)_n$ is convergent.
   If $s_n \to a$, one says that $\Sigma_n a_n$ *represents* $a \in F$ and sets $\Sigma_n a_n :\overset{\text{def}}{=} a$.
3) One says that $\Sigma_n a_n$ is absolutely convergent, if $\Sigma_n |a_n|$ is convergent.

Remark 6.13. Let $\Sigma_n a_n$ be a series. Even if $\Sigma_n a_n$ is convergent, one ***should not confuse*** the symbol $\Sigma_n a_n$ with the value $a \in F$ it represents.

Further, if $\Sigma_n a_n$ is convergent, then the sequence of partial sums $(s_n)_n$ is convergent, hence Cauchy, hence $a_n = s_n - s_{n-1} \to 0_F$ (WHY). In particular, one has the following (WHY):

Criterion 6.14. (Non-convergence of Series) *Let $\Sigma_n a_n$ be a series defined over F. If $a_n \not\to 0_F$, then $\Sigma_n a_n$ is not convergent.*

Definition 6.15. Let F be a totally ordered field, and consider $f(t) = \Sigma_n a_n t^n \in F[\![t]\!]$.

1) We say that $f(t)$ is (absolutely) convergent at $t = a \in F$, if the series $f(a) :\overset{\text{def}}{=} \Sigma_n a_n a^n$ is (absolutely) convergent.
2) Let $\Sigma_f := \{r \in F_{\geqslant 0} \mid \sum_n a_n t^n \text{ is abs. conv. } \forall\, x \in D_r(0)\}$. Then $D_f := \cup_{r \in \Sigma_f} D_r(0_f) \cup \{0_F\}$ is called the domain of (absolute) convergence of $f(t)$.
3) Recall that we denote $\infty := \sup(F_{\geqslant 0})$. With this conventional notation, one has:
   If $\rho_f := \sup(\Sigma_f) \cup \{\infty\}$ exists, then ρ_f is called the convergence radius of $f(t)$.

Remark 6.16. Note $f : D_f \to F$, $x \mapsto f(x)$, is a well defined map. If $D_f \neq \{0_F\}$, such maps, i.e., maps defined (around every point in the domain of definition) by power series, are called analytic maps. We will see later that the *elementary functions*, i.e., $\exp(x)$, $\sin(x)$, $\cos(x)$, $\log(x)$, the power functions x^α, are all analytic maps on their domains of definition.

7. The Field of Real Numbers $\mathbb{R}, +, \cdot, \leqslant$

As in the motivation for the introduction of the integer or the rational numbers, a simple reason why one needs a larger domain of numbers than $\mathbb{Q}$ is the fact that simple equations like $x^7 = 3$, or $10^x = 2$ have no solutions in $\mathbb{Q}$. The domain of numbers which contains $\mathbb{Q}$ and has almost all the desired properties is the

$$\textit{field of real numbers } \mathbb{R}, +, \cdot, \leqslant \ .$$

Moreover, it will turn out that $\mathbb{R}, +, \cdot, \leqslant$ is the unique field in which every bounded non-empty set X has a supremum and an infimum. The field of real numbers $\mathbb{R}$ is the basis of the *real analysis,* which is at the core modern science and engineering.

We will work in a more general context, in order to avoid repeating again and again definitions and constructions for both the totally ordered field of rational numbers $\mathbb{Q}, +, \cdot, \leqslant$ and subsequently for $\mathbb{R}, +, \cdot, \leqslant$. Hence we will consider a totally ordered field $F, +, \cdot, \leqslant$ and while working *in abstractum,* you can always think of $\mathbb{Q}$.

There are several constructions of $\mathbb{R}, +, \cdot, \leqslant$, and we will present two such constructions. The first invokes the notion of *convergence of sequences,* and it the construction via the *Cauchy sequences.* The second is the construction vie *Dedekind cuts.* Each construction has its own advantages, but in the end, the result of the construction is the same.

7.1. Construction of $\mathbb{R}$ via Cauchy sequences.

Let $F, +, \cdot, \leqslant$ be a totally ordered field, and $\mathcal{S}_{\mathrm{C}}(F)$ be the F-algebra of the Cauchy sequences. Define a relation $\sim$ on $\mathcal{S}_{\mathrm{C}}(F)$ by $(a_n)_n \sim (b_n)_n \overset{\text{def}}{\iff} a_n - b_n \to 0_F$.

Lemma 7.1. *The relation $\sim$ is an equivalence relation on $\mathcal{S}_{\mathrm{C}}(F)$.*

Proof. Let $(a_n)_n, (b_n)_n, (c_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$ be given. (i) $a_n - a_n \to 0_F$, hence $(a_n)_n \sim (a_n)_n$; (ii) $a_n - b_n \to 0_F$ iff $b_n - a_n \to 0_F$ (WHY). Hence $(a_n)_n \sim (b_n)_n \Rightarrow (b_n)_n \sim (a_n)_n$; (iii) $b_n - a_n \to 0_F$ & $c_n - b_n \to 0_F$, implies $c_n - a_n = (c_n - b_n) + (b_n - a_n) \to 0_F$ (WHY). Hence $(a_n)_n \sim (b_n)_n$ & $(b_n)_n \sim (c_n)_n \Rightarrow (a_n)_n \sim (c_n)_n$. □

Notations 7.2. In the above context, we introduce notations as follows:

1) For $\boldsymbol{a} = (a_n)_n$, let $\widehat{\boldsymbol{a}} :\overset{\text{def}}{=} \boldsymbol{a}/\!\sim = (a_n)_n/\!\sim$ denote the equivalence class of $\boldsymbol{a} = (a_n)_n$.
   Let $\widehat{F} := \mathcal{S}_{\mathrm{C}}(F)/\!\sim = \{\, \widehat{\boldsymbol{a}} \,|\, \boldsymbol{a} = (a_n)_n \in \mathcal{S}_{\mathrm{C}}(F) \,\}$ denote the set of equivalence classes.
2) For $a \in F$, let $\boldsymbol{a}_a$ be the a-constant sequence, and $\widehat{\boldsymbol{a}}_a \in \widehat{F}$ be its equivalence class.

Proposition 7.3. *The equivalence relation $\sim$ on $\mathcal{S}_{\mathrm{C}}(F)$ is compatible with addition and multiplication, i.e., if $\boldsymbol{a} = (a_n)_n \sim (a'_n)_n = \boldsymbol{a}'$ and $\boldsymbol{b} = (b_n)_n \sim (b'_n)_n = \boldsymbol{b}'$, then one has:*

$$(\boldsymbol{a} + \boldsymbol{b})/\!\sim = (\boldsymbol{a}' + \boldsymbol{b}')/\!\sim, \quad (\boldsymbol{a} \cdot \boldsymbol{b})/\!\sim = (\boldsymbol{a}' \cdot \boldsymbol{b}')/\!\sim, \quad (a \cdot \boldsymbol{a})/\!\sim = (a \cdot \boldsymbol{a}')/\!\sim \text{ for all } a \in F$$

In particular, the composition laws in $\mathcal{S}_{\mathrm{C}}(F)$ give rise to an addition $\oplus$, multiplication $\odot$, and multiplication by $a \in F$ on $\widehat{F} = \mathcal{S}_{\mathrm{C}}(F)/\!\sim$ such that the following hold:

1) *$\widehat{F}, \oplus, \odot$ is a commutative ring and an F-algebra, with $0_{\widehat{F}} = 0_{\mathcal{S}_{\mathrm{C}}(F)}/\!\sim$ and $1_{\widehat{F}} = 1_{\mathcal{S}_{\mathrm{C}}(F)}/\!\sim$. The map $\imath_F : F \to \widehat{F}$, $a \mapsto \widehat{\boldsymbol{a}}_a$ is injective and compatible with the composition laws.*
2) *Every $x \in \widehat{F}$, $x \neq 0_{\widehat{F}}$ is invertible w.r.t. $\odot$, hence $\widehat{F}$ is a field.*

Proof. Let $(a'_n)_n - (a_n)_n =: (a''_n)_n$ and $(b'_n)_n - (b_n)_n =: (b''_n)_n$ with $a''_n \to 0_F$, $b''_n \to 0_F$. Then one has:
Addition: $\big((a'_n)_n + (b'_n)_n\big) - \big((a_n)_n + (b_n)_n\big) = (a''_n)_n + (b''_n)_n = (a''_n + b''_n)_n$ with $a''_n + b''_n \to 0_F$ (WHY).
Multiplication: $\boldsymbol{a}' \cdot \boldsymbol{b}' - \boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{a}' \cdot \boldsymbol{b}' - \boldsymbol{a}' \cdot \boldsymbol{b} + \boldsymbol{a}' \cdot \boldsymbol{b} - \boldsymbol{a} \cdot \boldsymbol{b} = \boldsymbol{a}' \cdot (\boldsymbol{b}' - \boldsymbol{b}) + (\boldsymbol{a}' - \boldsymbol{a}) \cdot \boldsymbol{b} \to 0_F$ (WHY).
Multiplication by $a \in F$: $a \cdot \boldsymbol{a} - a \cdot \boldsymbol{a}' = a \cdot (\boldsymbol{a} - \boldsymbol{a}') = a \cdot (a''_n)_n = (a \cdot a''_n)_n$, and $a \cdot a''_n \to 0_F$ (WHY).
To 1): The fact that $\widehat{F}, \oplus, \odot$, is a commutative F-algebra follows directly form the definitions of $\oplus$, $\odot$ (HOW) (WHY) Make sure that you check all the details! Finally, $\imath_F(a+b) = \imath_F(a) \oplus \imath_F(b)$, $\imath_F(a \cdot b) = \imath_F(a) \odot \imath_F(b)$ are clear (WHY).
To 2): Let $x = (a_n)_n/\!\sim$. Then $x \neq 0_{\widehat{F}}$ implies that $a_n \not\to 0_F$ (WHY), hence w.l.o.g., $a_n \neq 0_F$ for all $n \in \mathbb{N}$ (WHY), and by Proposition 6.10, 4), b), $\big(\frac{1}{a_n}\big)_n$ is a Cauchy sequence (s.t. $\frac{1}{a_n} \not\to 0_F$). In particular, since $(a_n)_n \cdot \big(\frac{1}{a_n}\big)_n = 1_{\mathcal{S}(F)}$, it follows that setting $x' := \big(\frac{1}{a_n}\big)_n/\!\sim$, one has $x \cdot x' = 1_{\widehat{F}}$ (WHY). □

We next define a total ordering $\leqslant$ on $\widehat{F}$ which will turn out to be compatible with the composition laws and the embedding $\imath_F : F \to \widehat{F}$, that is, $a \leqslant b$ in F iff $\imath_F(a) \leqslant \imath_F(b)$ in $\widehat{F}$. Namely, let $\mathcal{S}_{\mathrm{C}}(F)_0$ be the subset of all the Cauchy sequences $\boldsymbol{a} = (a_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$ such that $\forall\, n \in \mathbb{N}$ one has $a_n \geqslant 0_F$. $\mathcal{S}_{\mathrm{C}}(F)_0$ is a semiring, i.e., it is closed w.r.t. addition and multiplication, and $0_{\mathcal{S}_{\mathrm{C}}(F)}, 1_{\mathcal{S}_{\mathrm{C}}(F)} \in \mathcal{S}_{\mathrm{C}}(F)_0$ (WHY).

Proposition 7.4. *In the above notation, let $\widehat{F}_0 :\overset{\text{def}}{=} \mathcal{S}_{\mathrm{C}}(F)_0/\!\sim$. The following hold:*
1) *$\widehat{F}_0 \subset \widehat{F}$ is a semifield, i.e., it is closed w.r.t. addition, multiplication, $0_{\widehat{F}}, 1_{\widehat{F}} \in \widehat{F}_0$, and every $x \in \widehat{F}_0$, $x \neq 0_{\widehat{F}}$ has its inverse x^{-1} in $\widehat{F}_0$.*
2) *One has $\widehat{F} = -\widehat{F}_0 \cup \widehat{F}_0$ and $-\widehat{F}_0 \cap \widehat{F}_0 = \{0_{\widehat{F}}\}$.*

Hence $x \leqslant y \overset{\text{def}}{\longleftrightarrow} y - x \in \widehat{F}_0$ is a total ordering on $\widehat{F}$ compatible with $\oplus$ and $\odot$. Moreover, $\imath_F : F \to \widehat{F}$ is compatible with ordering, i.e., $a \leqslant b$ in F iff $\imath_F(a) \leqslant \imath_F(b)$ in $\widehat{F}$.

Proof. To 1): Since $\mathcal{S}_{\mathrm{C}}(F)_0$ is closed w.r.t. addition and multiplication, it follows that $\widehat{F}_0$ is closed w.r.t. addition and multiplication (WHY), and obviously one has that $0_{\widehat{F}}, 1_{\widehat{F}} \in \widehat{F}_0$ (WHY). Finally, if $x \in \widehat{F}_0$ satisfies $x \neq 0_{\widehat{F}}$, then $x = \boldsymbol{a} = (a_n)_n/\!\sim$ with $a_n \geqslant 0_F$, and $a_n \not\to 0_F$ (WHY). Hence by Proposition 6.10, 4), b), there is $\epsilon > 0_F$ and $N \in \mathbb{N}$ s.t. $\epsilon < a_n$ for $n > N$ (WHY). Hence setting $\boldsymbol{a}' := (a'_n)_n$ with $a'_n = 1_F$ for $n \leqslant N$ and $a'_n = a_n$ for $n > N$, it follows that $\widehat{\boldsymbol{a}} = \widehat{\boldsymbol{a}}'$ (WHY), $\boldsymbol{a}' \in \mathcal{S}_{\mathrm{C}}(F)_0$, and by Proposition 6.10, 4), b), $\big(\frac{1}{a'_n}\big)_n \in \mathcal{S}_{\mathrm{C}}(F)_0$.
Finally, since $(a'_n)_n \cdot \big(\frac{1}{a'_n}\big)_n = 1_{\mathcal{S}(F)}$, one has: $\big(\frac{1}{a'_n}\big)_n/\!\sim$ is the inverse of $\widehat{\boldsymbol{a}}' = \widehat{\boldsymbol{a}} = x$ with respect to $\cdot$ in $\widehat{F}$.
To 2): Let $\boldsymbol{a} = (a_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$ be given. First, if $a_n \to 0_F$, then $(a_n)_n \sim 0_{\mathcal{S}_{\mathrm{C}}(F)}$, and $0_{\mathcal{S}_{\mathrm{C}}(F)} \in \mathcal{S}_{\mathrm{C}}(F)_0$. Second, if $a_n \not\to 0_F$, by Proposition 6.10, 4), b), one has: $\exists\, \epsilon > 0_F, N \in \mathbb{N}$ s.t. either $a_n < -\epsilon$, or $\epsilon < a_n$ for all $n > N$. Set $\boldsymbol{a}' := (a'_n)_n$ with $a'_n = 0_R$ for $n \leqslant N$ and $a'_n = a_n$ for $n > N$. Then $\boldsymbol{a} \sim \boldsymbol{a}'$ (WHY), and either $\boldsymbol{a}'$ or $-\boldsymbol{a}'$, **but not both**, lies in $\mathcal{S}_{\mathrm{C}}(F)_0$. In particular, $\widehat{\boldsymbol{a}} \in \widehat{F}_0$ iff $-\widehat{\boldsymbol{a}} \notin \widehat{F}_0$ (WHY), concluding that $\widehat{F} = -\widehat{F}_0 \cup \widehat{F}_0$, $-\widehat{F}_0 \cap \widehat{F}_0 = \{0_{\widehat{F}}\}$ (WHY). Thus by Proposition 5.21, $\widehat{F}, \oplus, \odot, \leqslant$ is a totally ordered field. Finally, to prove that $\imath_F$ is compatible with orderings, notice that for $a \in F$, the a-constant sequence $\boldsymbol{a}_a := (a)_n$ lies in $\mathcal{S}_{\mathrm{C}}(F)_0$ iff $a \geqslant 0_F$ iff $\imath_F(a) \in \widehat{F}_0$ (WHY). Hence $a \leqslant b$ in F iff $b - a \geqslant 0_F$ iff $\imath(b-a) \in \widehat{F}_0$ iff $\imath_F(a) \leqslant \imath_F(b)$ (WHY). □

Convention/Definition 7.5. Let $F,+,\cdot,\leqslant$ be a totally ordered field, and $\imath_F : F \to \widehat{F}$ be the canonical embedding defined in Proposition 7.4.

1) We denote the addition $\oplus$ and multiplication $\odot$ in $\widehat{F}$ simply by $+,\cdot$.
   Further, we identify F with $\imath_F(F)$, hence consider $F,+,\cdot,\leqslant$ as a subfield of $\widehat{F},+,\cdot,\leqslant$.
2) We say $F,+,\cdot,\leqslant$ is *complete,* if every Cauchy sequence $(a_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$ is convergent in F, or equivalently, one has that $\mathcal{S}_{\mathrm{C}}(F) = \mathcal{S}_{\mathrm{c}}(F)$.

Theorem 7.6. *For a totally ordered field $F,+,\cdot,\leqslant$, consider $\widehat{F},+,\cdot,\leqslant$ and the embedding of totally ordered fields $F \hookrightarrow \widehat{F}$ defined above. The following hold:*

1) *F is dense in $\widehat{F}$, i.e, for every $x<y$ in $\widehat{F}$ there is $a \in F$ such that $x<a<y$.*
2) *For $\boldsymbol{a} := (a_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$ one has $a_n \to \widehat{\boldsymbol{a}}$ in $\widehat{F}$, and the field $\widehat{F}$ is complete.*
3) *$F \hookrightarrow \widehat{F}$ is an isomorphism iff F is complete, or equivalently, $F = \widehat{F}$.*

Terminology. *$\widehat{F}$ together with the identification $\imath_F : F \to \widehat{F}$ is the **completion** of F.*

Proof. **To 1)**: Let $x = (a_n)_n/\!\sim$, $y = (b_n)_n/\!\sim$. Since $x<y$ one has $y-x \in \mathcal{F}_0$, $y-x \neq 0_{\widehat{F}}$. Hence by definitions one has: $y-x = (b_n-a_n)_n/\!\sim = (c_n)_n/\!\sim$ for some $(c_n)_n \in \mathcal{S}_{\mathrm{C}}(F)_0$ such there is $\epsilon > 0_F$ and $N_0 \in \mathbb{N}$ such that for all $n > N_0$ one has $c_n > \epsilon$. Since $(a_n)_n$ and $(b_n)_n$ are Cauchy, for $\epsilon' := \frac{1}{4}\epsilon$, there is $N' \in \mathbb{N}$ s.t. for $m,n > N'$ one has: $(*)$ $\epsilon' < b_n - b_m, a_n - a_m < \epsilon'$ (WHY). Hence setting $a := \frac{1}{2}(b_N + a_N)$, for $N > N', N_0$ one has: (i) Since $b_N - a_N > \epsilon > 0_F$, one has $b_N + a_N > \epsilon + 2a_N > 2a_N$ (WHY), hence $a > \frac{1}{2}\epsilon + a_N$ (WHY). (ii) Since $b_N \overset{\text{why}}{=} \frac{1}{2}(b_N - a_N) + \frac{1}{2}(b_N + a_N)$, one has $b_N - \frac{1}{2}\epsilon > a$. We claim that $b_n > \frac{1}{4}\epsilon + a$ and $a - \frac{1}{4}\epsilon > a_n$ for all $n > N$. Indeed, since by $(*)$ one has $-\frac{1}{4}\epsilon < b_n - b_N, a_n - a_N < \frac{1}{4}\epsilon$ for $n \geqslant N$, one has:

$$a_n = (a_n - a_N) + a_N < \tfrac{1}{4}\epsilon + a_N < a - \tfrac{1}{4}\epsilon, \quad b_n = (b_n - b_N) + b_N > -\tfrac{1}{4}\epsilon + b_N > a + \tfrac{1}{4}\epsilon \quad \text{(WHY)}.$$

Let $\boldsymbol{a}' = (a'_n)_n$, $\boldsymbol{b}' = (b_n)_n$ with $a'_n = a_n$, $b'_n = b_n$ for $n > N$ and $a_n = a = b_n$ for $n \leqslant N$. Then $\boldsymbol{a}' \sim \boldsymbol{a}$, $\boldsymbol{b}' \sim \boldsymbol{b}$ (WHY), hence $x = \widehat{\boldsymbol{a}}'$, $y = \widehat{\boldsymbol{b}}'$ (WHY), and obviously, $x \leqslant a - \frac{1}{4} < a < a + \frac{1}{4} \leqslant y$ (WHY).

To 2): First, by assertion 1), $\forall \epsilon_{\widehat{F}} > 0_{\widehat{F}}$ in $\widehat{F}$, there is $\epsilon > 0_F$ in F s.t. $0_{\widehat{F}} < \epsilon < \epsilon_{\widehat{F}}$ in $\widehat{F}$. Hence to test whether $(x_n)_n \in \mathcal{S}_{\mathrm{c}}(\widehat{F})$ or $(x_n)_n \in \mathcal{S}_{\mathrm{C}}(\widehat{F})$, it's enough to use $\epsilon \in F_{>0}$ (and not all $\epsilon_{\widehat{F}} \in \widehat{F}_{>0}$). **(Check details!)**

Let $\boldsymbol{a} = (a_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$ be given. By the min/max construction 6.6 there is a subsequence $(a_{n_k})_k$ which either constant or strictly monotone. By Proposition 6.10, 3), 2), one has: $(a_{n_k})_k \in \mathcal{S}_{\mathrm{c}}(\widehat{F})$, and $a_n \to \widehat{\boldsymbol{a}}$ iff $a_{n_k} \to \widehat{\boldsymbol{a}}$ (WHY). Hence w.l.o.g., we can replace $(a_n)_n$ by $(a_{n_k})_k$, thus suppose that $(a_n)_n$ is either constant, or strictly monotone. If $(a_n)_n$ is constant, say $a_n = a$ for $n \gg 0$, then $a_n \to a \in \widehat{F}$ (WHY). Next let $(a_n)_n$ be strictly monotone, say strictly increasing (to fix notations), that is $a_n < a_{n+1}$ for $n \in \mathbb{N}$. We show that $a_m \to \widehat{\boldsymbol{a}}$. Indeed, let $\epsilon > 0_F$ be given. Then $(a_n)_n$ being Cauchy implies: $0_F \leqslant a_n - a_m \leqslant \epsilon$ for $n > m \gg 0$ (WHY). Hence setting $(b_n)_n := (a_n - a_m)_n, (c_n)_n := (\epsilon + a_m - a_n)_n$ one has $(b_n)_n, (c_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$ (WHY), and $(b_n)_n/\!\sim = \widehat{\boldsymbol{a}} - a_m$, $(c_n)_n/\!\sim = \epsilon + a_m - \widehat{\boldsymbol{a}} = \epsilon - (\widehat{\boldsymbol{a}} - a_m)$ (WHY). Further, since $0_F \leqslant a_n - a_m \leqslant \epsilon$ for $n > m$, one has $0_{\widehat{F}} \leqslant \widehat{\boldsymbol{a}} - a_m, \epsilon - (\widehat{\boldsymbol{a}} - a_m)$ (WHY). Hence $0_{\widehat{F}} \leqslant \widehat{\boldsymbol{a}} - a_m \leqslant \epsilon$ for all $m \gg 0$ (WHY). Conclude that $a_m \to \widehat{\boldsymbol{a}}$ in $\widehat{F}$ (WHY). Complete the proof for $(a_n)_n$ decreasing (**Ex** ...).

Finally, to prove that $\widehat{F}$ is complete, we prove that every Cauchy sequence $(x_n)_n \in \mathcal{S}_{\mathrm{c}}(\widehat{F})$ is convergent. First, given $(x_n)_n \in \mathcal{S}_{\mathrm{C}}(\widehat{F})$, arguing as above in the case of $(a_n)_n$, the convergence of $(x_n)_n$ in $\widehat{F}$ is reduced to the case that $(x_n)_n$ is strictly monotone, say $(x_n)_n \nearrow$ (WHY). Then by assertion 1), for every $n \in \mathbb{N}$ $\exists a_n \in F$ s.t. $x_n < a_n < x_{n+1}$, hence $a_n < x_{n+1} < a_{n+1}$. In particular, the resulting $(a_n)_n \in \mathcal{S}(F)$ is strictly monotone and Cauchy (WHY), hence $a_n \to \widehat{\boldsymbol{a}}$ in $\widehat{F}$ (WHY). Prove that $x_n \to \widehat{\boldsymbol{a}}$ in $\widehat{F}$ (**Ex** ...). The case $(x_n)_n \searrow$ is **Ex** ...

To 3): After identifying F with $\imath_F(F) \subset \widehat{F}$, one has to prove that $F = \widehat{F}$ iff F is complete. Since $\widehat{F}$ is complete by assertion 2), one has: If $F = \widehat{F}$, then F ic complete (because $\widehat{F}$ is so). Second, if F is complete, then $\mathcal{S}_{\mathrm{c}}(F) = \mathcal{S}_{\mathrm{C}}(F)$, hence for every $(a_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$ there is $a \in F$ s.t. $a_n \to a$. In particular, $a_n - a \to 0_F$, hence $(a_n) \sim (a)_n$, concluding that $\widehat{\boldsymbol{a}} = a \in F$. Hence $\widehat{F} = F$. □

Definition/Remark 7.7. For the totally ordered field $\mathbb{Q}, +, \cdot, \leqslant$ we consider/define:

1) Denote $\mathbb{R} := \widehat{\mathbb{Q}} = \mathcal{S}_C(\mathbb{Q})/\sim$ and call $\mathbb{R}, +, \cdot, \leqslant$ the field of real numbers.
   In particular, $\mathbb{R} = \widehat{\mathbb{R}}$ is complete, i.e., every Cauchy sequences in $\mathbb{R}$ is convergent in $\mathbb{R}$.
2) Under the embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$, one has $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ compatibly with addition, multiplication, and ordering, such that $0 = 0_{\mathbb{Z}} = 0_{\mathbb{Q}} = 0_{\mathbb{R}}$ and $1 = 1_{\mathbb{Z}} = 1_{\mathbb{Q}} = 1_{\mathbb{R}}$.

7.2. Characterization of $\mathbb{R}, +, \cdot, \leqslant$.

In this subsection we characterize $\mathbb{R}, +, \cdot, \leqslant$ among all totally ordered fields.

Definition/Remark 7.8. Let $F, +, \cdot, \leqslant$ be a totally ordered field. TFAE:

(i) F satisfies the Archimedean Axiom, i.e., $\forall\, x \in F, \epsilon > 0_F$, $\exists\, n \in \mathbb{N}$ s.t. $x < n\epsilon$.
(ii) $\frac{1}{n} \to 0_F$; (ii)′ The set $\mathbb{N}\,1_F := \{n1_F \,|\, n \in \mathbb{N}\}$ is unbounded.
(iii) For $x < y$ in F there is $\frac{a}{r} \in \mathbb{Q}$ such that $x < \frac{a}{r}\,1_F < y$, i.e., $\mathbb{Q}$ is dense in F.

We say that $F, +, \cdot, \leqslant$ is Archimedean, it F satisfies the conditions (i), (ii), (iii).

Ex 7.9. Show that the above conditions (i), (ii), (iii) are equivalent.

Definition/Remark 7.10. Let $F, +, \cdot, \leqslant$ be a totally ordered field, and $X \subset F$ denote non-empty sets. The following conditions are equivalent:

(i) Every X bounded above has $\sup(X)$ in F.
(ii) Every X bounded below has $\inf(X)$ in F.
(iii) Every X which is bounded has $\in (X)$ and $\sup(X)$ in F.

We say that a totally ordered field $F, +, \cdot, \leqslant$ satisfies the Completeness Axiom, if it satisfies conditions (i), (ii), (iii).

Ex 7.11. Show that the above conditions (i), (ii), (iii) are equivalent.

Theorem 7.12 (Characterizations of $\mathbb{R}$).
For a totally ordered field $F, +, \cdot, \leqslant$ the following condition are equivalent:

(i) *$F = \mathbb{R} = \widehat{\mathbb{Q}}$ is the completion of $\mathbb{Q}$.*
(ii) *F is an Archimedean complete field.*
(iii) *F satisfies the Completion Axiom.*

Hence $\mathbb{R}$ is the only field which is Archimedean complete or satisfies the Completness Axiom.

Proof. (i) $\Rightarrow$ (ii): Clear, because $\mathbb{R} = \widehat{\mathbb{Q}}$ is Archimedean and complete (WHY). (ii) $\Rightarrow$ (i): We show that $\forall\, x \in F$ there is $(a_n)_n \in \mathcal{S}_C(\mathbb{Q})$ s.t. $a_n \to x$, hence $x \in \widehat{\mathbb{Q}} = \mathbb{R}$, thus $F = \mathbb{R}$ by the fact that F is complete. Now, since $\mathbb{Q}1_F$ is dense in F one has: $\forall\, n \in \mathbb{N}_{>0}$ $\exists\, a_n \in \mathbb{Q}$ s.t. $-\frac{1}{n} + x < a_n < x$ (WHY). Hence $x - a_n \to 0_F$ (WHY), and therefore $a_n \to x$ in F (WHY), as claimed.

(i) $\Rightarrow$ (iii): Let $X \subset \mathbb{R}$ be a non-empty bounded above subset. We prove that $\sup(X)$ exists in $\mathbb{R}$. Since $\mathbb{Z} \subset \mathbb{R}$ is unbounded below and above (WHY), there is $a \in \mathbb{Z}$ minimal s.t. $\forall\, x \in X$ one has $x < a + 1$, and $\exists\, x \in X$ s.t. $a \leqslant x$. Construct inductively $(a_n)_n \nearrow$ and $(b_n)_n \searrow$ s.t. $a_0 := a$, $b_0 = a + 1$, $b_n = a_n + \frac{1}{2^n}$, and further: $\exists\, x_n \in X$ s.t. $a_n \leqslant x_n < b_n$, and $x' < b_n$ for all $x' \in X$. Indeed, if a_n, b_n are constructed, consider $c_n := \frac{1}{2}(a_n + b_n)$, and further do: First, if $\exists\, x_{n+1} \in X$ s.t. $c_n \leqslant x_{n+1}$, then set $a_{n+1} = c_{n+1}$, $b_{n+1} := b_n$, and note that $x_{n+1} < b_{n+1}$ (WHY). Second, if $\forall\, x' \in X$ one has $x' < c_n$, set $a_{n+1} := a_n$, $b_{n+1} := c_n$, $x_{n+1} := x_n$, and note that $x_{n+1} < b_{n+1}$ (WHY). Finally, since $b_n - a_n = \frac{1}{2^n} \to 0$ (WHY), one has $(a_n)_n, (b_n)_n \in \mathcal{S}_C(\mathbb{R})$ (WHY). Hence $\exists\, c \in \mathbb{R}$ with $a_n \to c \leftarrow b_n$, thus $x_n \to c$ (WHY). Further $x = \sup(X)$ (WHY).

(iii) $\Rightarrow$ (ii): Let F satisfy the Completeness Axiom. First, we claim that $X := \mathbb{N}1_F$ is unbounded in F, hence F is Archimedean. Indeed, by contradiction, suppose that $\mathbb{N}1_F$ is bounded, and let $x_{\mathbb{N}} := \sup(X)$. Then $n1_F < x_{\mathbb{N}}$ for all $n \in \mathbb{N}$, and if $n1_F < x'$ for all $n \in \mathbb{N}$, then $x_{\mathbb{N}} \leqslant x'$. OTOH, since $(n+1)1_F < x_{\mathbb{N}}$, one has $n1_F < x_{\mathbb{N}} - 1_F$ for all $n \in \mathbb{N}$ (WHY), and clearly, $x' := x_{\mathbb{N}} - 1 < x_{\mathbb{N}}$ (WHY), **contradiction!**. Second, we claim that F is complete. Indeed, it is sufficient to prove that every strictly increasing sequence $(x_n)_n \in \mathcal{S}_{\mathrm{C}}(F)$ is convergent in F (WHY). Let $X = \{x_n \,|\, n \in \mathbb{N}\}$, and $x := \sup(X)$. Then $x_n \to x$ (WHY). □

7.3. The topology of the field of real numbers $\mathbb{R}$.

The *topology* on $\mathbb{R}$ (and more general, on any non-empty set X, as we will define it later) is about defining and working rigorously with the notion of "proximity" (Google it!).

Definition 7.13 (Intervals). Consider $a \leqslant b$ in $\mathbb{R}$, and define the intervals in $\mathbb{R}$ as follows:

1) The open intervals are subsets of $\mathbb{R}$ of the form:
$(a,b) := \{x \in \mathbb{R} \,|\, a < x < b\}$; $(-\infty, a) := \{x \in \mathbb{R} \,|\, x < a\}$; $(a, \infty) := \{x \in \mathbb{R} \,|\, a < x\}$.
2) The closed intervals are subsets of $\mathbb{R}$ of the form:
$[a,b] := \{x \in \mathbb{R} \,|\, a \leqslant x \leqslant b\}$; $(-\infty, a] := \{x \in \mathbb{R} \,|\, x \leqslant a\}$; $[a, \infty) := \{x \in \mathbb{R} \,|\, a \leqslant x\}$.
3) The open-closed, respectively closed-open intervals are subsets of $\mathbb{R}$ of the form:
$(a,b] := \{x \in \mathbb{R} \,|\, a < x \leqslant b\}$, respectively $[a,b) := \{x \in \mathbb{R} \,|\, a \leqslant x < b\}$.

Notation. For $x \in \mathbb{R}$ and $\epsilon > 0$, we denote:

- $B_\epsilon(x) := \{x' \in \mathbb{R} \,\big|\, |x - x'| < \epsilon\} = (-\epsilon + x, x + \epsilon)$, called the open ball of center x and radius ϵ.
- $\overline{B}_\epsilon(x) := \{x' \in \mathbb{R} \,\big|\, |x - x'| \leqslant \epsilon\} = [-\epsilon + x, x + \epsilon]$, called the closed ball of center x and radius ϵ.

Definition 7.14 (Open/Closed Subsets). Let $U \subset \mathbb{R}$ and $A \subset \mathbb{R}$ denote subsets.

1) $U \subset \mathbb{R}$ is called open, if either $U = \emptyset$, or $\forall\, x \in U\ \exists\, \epsilon > 0$ s.t. $B_\epsilon(x) \subset U$.
2) $A \subset \mathbb{R}$ is called closed, if its complement $\complement_{\mathbb{R}}(A)$ in $\mathbb{R}$ is open.

Ex 7.15. Prove the following:

1) Open intervals are open subsets, and $U \subset \mathbb{R}$ is open iff U is a union of open intervals.
2) A subset $A \subset \mathbb{R}$ is closed iff A is an intersection of complements of open intervals. In particular, closed intervals are closed sets.

Proposition 7.16 (Basics about Topology). *The following hold:*

1) *The open sets in $\mathbb{R}$ have the properties:*
   (i) *$\emptyset$ and $\mathbb{R}$ are open sets.*
   (ii) *If U_i, $i \in I$ arbitrary, are open sets in $\mathbb{R}$, then $\cup_i U_i$ is open.*
   (iii) *If U_i, $i \in I$ finite, are open sets of $\mathbb{R}$, then $\cap_i U_i$ is open.*

   Terminology. *The set $\tau_{\mathbb{R}} \overset{\text{def}}{:=} \{U \subset \mathbb{R} \,|\, U \text{ is open}\} \subset \mathcal{P}(\mathbb{R})$ is called the topology of $\mathbb{R}$.*
2) *The closed sets in $\mathbb{R}$ have the properties:*
   (i)′ *$\emptyset$ and $\mathbb{R}$ closed sets.*
   (ii)′ *If A_i, $i \in I$ arbitrary, are closed sets in $\mathbb{R}$, then $\cap_i A_i$ is closed.*
   (iii)′ *If A_i, $i \in I$ finite, are closed sets in $\mathbb{R}$, then $\cup_i A_i$ is closed.*

Proof. To 1), (i): **Ex**... To (ii): Let $x \in \cup_i U_i$ be given. Then $\exists\, i_x \in I$ s.t. $x \in U_{i_x}$ (WHY). Since U_{i_x} is open, $\exists\, \epsilon > 0$ s.t. $B_\epsilon(x) \subset U_{i_x}$, thus $B_\epsilon(x) \subset U_{i_x} \subset \cup_i U_i$ (WHY). Conclude that $\cup_i U_i$ is open. To (iii): Let $x \in \cap_i U_i$. Then $x \in U_i$ for all $i \in I$, and since U_i are open, one has: $\exists\, \epsilon_i > 0$ s.t. $B_{\epsilon_i}(x) \subset U_i$. Since I is finite, $\epsilon := \min\{\epsilon_i \,|\, i \in I\}$ exists and $\epsilon > 0$ (WHY). Further, since $\epsilon \leqslant \epsilon_i$, one has $B_\epsilon(x) \subset B_{\epsilon_i}(x)$ (WHY), hence $B_\epsilon(x) \subset U_i$ for all $i \in I$. Thus $B_\epsilon(x) \subset \cap_i U_i$ (WHY). Conclude that $\cap_i U_i$ is open.

To 2): **Ex** (**Hint**: Use de Morgan laws: If X_i, $i \in I$ are subsets of X, then $\complement_X(\cup_i X_i) = \cap_i \complement_X(X_i)$, and $\complement_X(\cap_i X_i) = \cup_i \complement_X(X_i)$, and take into account that $A_i \subset \mathbb{R}$ is closed iff $U_i := \complement_{\mathbb{R}}(A_i)$ is open, etc....) □

Definition 7.17 (Neighborhoods/Closure/Interior). For $x \in \mathbb{R}$ and $X \subset \mathbb{R}$ we define:

1) A neighborhood of $x \in \mathbb{R}$ is any subset $U_x \subset \mathbb{R}$ s.t. $\exists\, \epsilon > 0$ with $B_\epsilon(x) \subset U_x$.
   Notation: $\tau_{\mathbb{R},x} \subset \mathcal{P}(\mathbb{R})$ is the set of all neighborhoods of x.
   We say that $x \in X$ is isolated in X, if $\exists\, \epsilon > 0$ s.t. $B_\epsilon(x) \cap X = \{x\}$.
   If $x \in X$ is not isolated in X, we say that x is an accumulation point of X.
2) We say that $x \in \mathbb{R}$ is in the closure of X, if $\forall\, \epsilon > 0$ one has: $B_\epsilon(x) \cap X$ is non-empty.
   Notation. $\overline{X} := \{x \in \mathbb{R} \,|\, x$ lies in the closure of $X\}$ is called the closure of X.
3) We say that $x \in \mathbb{R}$ lies in the interior of X, if $\exists\, \epsilon > 0$ s.t. $B_\epsilon(x) \subset X$.
   Notation. $\overset{\circ}{X} := \{x \in \mathbb{R} \,|\, x$ is interior point of $X\}$ is called the interior of X.

Example 7.18. The following hold:

a) $[0,1)$ is neighborhood of all $x = \frac{1}{2}$, but not of $x = 0$ (WHY); and of all x with $0 < x < 1$ (WHY).
   All points in $X = [0,1)$ are accumulation points (WHY).
b) The closure of $X = [0,1)$ is $[0,1]$ (WHY).
   Actually, the closure of any interval is the closed interval with the same extremities (WHY).
c) The interior of $X = [0,1)$ is $(0,1)$ (WHY).
   Actually, the interior of any interval is the open interval with the same extremities (WHY).
d) If $x_n \to x$ and $X = \{x_n \,|\, n \in \mathbb{N}\}$ is the set of values, then $\overline{X} = X \cup \{x\}$ (WHY) and $\overset{\circ}{X} = \emptyset$ (WHY).
   Further, if $x \in \overline{X}$ isolated iff $(x_n)_n$ is not almost constant (WHY).
e) If $U \subset \mathbb{R}$ is open non-empty, and $X = U \cap \mathbb{Q}$, then $\overline{X} = \overline{U}$ (WHY), and $\overset{\circ}{X} = \emptyset$ (WHY).
   Further, all points of X are accumulation points (WHY).

Proposition 7.19 (Basics about Interior/Closure of Sets). *The following hold:*

1) *$X \subset \mathbb{R}$ is open iff $X \in \tau_{\mathbb{R},x}$ for all $x \in X$ iff $X = \overset{\circ}{X}$, i.e., X equals its interior.*
2) *$X \subset \mathbb{R}$ is closed iff $X = \overline{X}$ iff every $(x_n)_n \in \mathcal{S}_{\mathrm{C}}(X)$ has limit $x_n \to x \in X$.*
   Further, all points in $x \in \overline{X} \setminus X$ are accumulation points.

Proof. To 1): U is open $\overset{\text{def}}{\longleftrightarrow}$ $\forall\, x \in U\ \exists\, \epsilon_x > 0$ s.t. $B_{\epsilon_x}(x) \subset U$ iff $\forall\, x \in U$ one has $x \in \overset{\circ}{U}$ iff $U = \overset{\circ}{U}$.
To 2): X is closed $\overset{\text{def}}{\longleftrightarrow}$ $U := \complement_{\mathbb{R}}(X)$ is open iff $\forall\, x \notin X$ one has $U \in \tau_{\mathbb{R},x}$ iff all $x \notin X \Rightarrow x \notin \overline{X}$ (WHY). Next let $x_n \to x$ with $x_n \in X$. Then $\forall\, \epsilon > 0$ one has $x_n \in B_\epsilon(x)$ for $n \gg 0$ (WHY). Hence $B_\epsilon(x) \cap X \neq \emptyset$, implying that $x \in \overline{X} = X$. Conversely, if $x \notin \overline{X} = X$, then there is $\epsilon > 0$ s.t. $B_\epsilon(x) \cap X = \emptyset$, hence there is no sequence $x_n \to x$ with $x_n \in X$ (WHY). Finally, for the last assertion, let $x \in \overline{X} \setminus X$ be given. By contradiction, suppose that x is not accumulation point for $\overline{X}$, hence by definition, $\exists\, \epsilon > 0$ s.t. $B_\epsilon(x) \cap \overline{X} = \{x\}$. Since $x \in \overline{X} \setminus X$, one has $B_\epsilon(x) \cap X = \emptyset$ (WHY), thus $x \notin \overline{X}$, Ctr!!! □

Definition 7.20 (Connectedness). Let $X \subset \mathbb{R}$ be a non-empty set.

1) X is called disconnected if there are $U_1, U_2 \subset \mathbb{R}$ open disjoint s.t. $X \subset U_1 \cup U_2$, $X \cap U_1 \neq \emptyset \neq X \cap U_2$.
2) X is called connected if it is not disconnected, i.e., for any disjoint open subsets U_1, U_2 such that $X \subset U_1 \cup U_2$ one has: *either* $X \subset U_1$, *or* $X \subset U_2$.

Example 7.21. Intuitively, a subset $X \subset \mathbb{R}$ is connected if X consists of "one piece."

a) $X = [0, 1)$ is connected (WHY). Actually, every interval is connected (WHY).
b) $X = \cup_n (n, n+1)$ is disconnected.
c) $X = \{0, 1\}$ is disconnected (WHY).
Actually, every finite set X with $|X| > 1$ is disconnected (WHY).
d) If $X \subset \mathbb{Q}$, then X is connected iff $|X| = 1$ (WHY).
e) If $X, Y \subset \mathbb{R}$ are non-empty and disjoint, then $X \cup Y$ is disconnected.

Proposition 7.22 (Basics about Connectedness). *The following hold:*

1) *A non-empty subsets $X \subset \mathbb{R}$ is connected iff X is an interval in $\mathbb{R}$.*
2) *In particular, one has:*
   a) *If X is finite, then X is connected iff $|X| = 1$.*
   b) *If X is infinite and connected, then $\overline{X}$ and $\overset{\circ}{X}$ are connected.*
   c) *If $X, Y \subset \mathbb{R}$ are connected and $X \cap Y \neq \emptyset$, then $X \cup Y$ is connected.*

Proof. To 1): "$\Rightarrow$" First we notice that a subset $Y \subset \mathbb{R}$ is an interval iff $\forall\, a, b \in Y$ with $a \leqslant b$ one has: $[a, b] \subset X$ (WHY). Hence to prove that X is an interval, we have to prove that $\forall\, a, b \in X$ with $a \leqslant b$ one has: $[a, b] \subset X$. By contradiction, suppose that $[a, b] \not\subset X$, that is, $\exists\, x \in \mathbb{R}$ with $a < x < b$ and $x \notin X$. Then setting $U_1 := (-\infty, x)$, $U_2 := (x, \infty)$, one has: $X \subset \mathbb{R}\backslash\{x\} = U_1 \cup U_2$ (WHY), $U_1 \cap U_2 = \emptyset$, and $a \in X \cap U_1$, $b \in X \cap U_2$. Hence by definition one has that X is not connected, Ctr!!!
"$\Leftarrow$" Let X be an interval in $\mathbb{R}$, and U_1, U_2 be disjoint open subsets such that $X \subset U_1 \cup U_2$. We prove that either $X \subset U_1$, or $X \subset U_2$. By contradiction, suppose that $X \subset U_1, X \cap U_2 \neq \emptyset$. Choose $a \in X \cap U_1$, $b \in X \cap U_2$, and w.l.o.g., let $a \leqslant b$, hence $a < b$ (WHY). Hence since U_1, U_2 are open, $\exists\, \epsilon > 0$ s.t. $B_\epsilon(a) \subset U_1$, $B_\epsilon(b) \subset U_2$ (WHY), hence $[a, a + \epsilon] \subset U_1$, $[-\epsilon + b, b] \subset U_2$. Let $X_1 := [a, b] \cap U_1$. Then $X_1 \neq \emptyset$ (WHY)and $b' := -\epsilon + b$ is an upper bound of X_1 (WHY). Hence by the Completeness Axiom, $x := \sup(X_1)$ exists in $\mathbb{R}$, and $a + \epsilon \leqslant x \leqslant -\epsilon + b$ (WHY). Hence since $[a, b] \subset X \subset U_1 \cup U_2$ (WHY), it follows that either $x \in U_1$, or U_2. First, if $x \in U_1$ one has: Since U_1 and is open and $x \in U_1$, $\exists\, \epsilon > 0$ s.t. $B_\epsilon(x) \subset U_1$, hence all $x < x' < x + \epsilon$ lie in $U_1 \cap [a, b]$ (WHY). Thus $x' \in X_1$, contradicting that $x = \sup(X_1)$. Second, if $x \in U_2$, one has: Since U_2 is open $x \in U_2$, $\exists\, \epsilon > 0$ s.t. $B_\epsilon(x) \subset U_2$, hence all x'' with $-\epsilon + x < x'' < x$ lie in $U_2 \cap [a, b]$ (WHY). OTHO, since $x = \sup(X_1)$ and $x'' < x = \sup(X)$, there must exist $x' \in X_1$ with $x'' < x' \leqslant x$ (WHY). Hence $x' \in (-\epsilon + x, x] \subset U_2$, i.e., $x' \in U_1 \cap U_2$, Ctr!!!, because $U_1 \cap U_2 = \emptyset$. To 2): **Ex**... □

Definition/Remark 7.23 (Compactness). Let $X \subset \mathbb{R}$ denote *non-empty* subsets. An open covering of X is any family of open subsets $(U_i)_{i \in I}$ such that $X \subset \cup_{i \in I} U_i$. A subcovering of $(U_i)_{i \in I}$ is a covering of the form $(U_i)_{i \in I'}$ for some subset $I' \subset I$. Consider the condition:

(i) We say that X has the finite covering property, if for every open covering $(U_i)_{i \in I}$ of X, there is $I' \subset I$ finite s.t. $X \subset \cup_{i' \in I'} U_{i'}$.
(ii) We say that X has the finite intersection property, if for every family of closed sets $(A_i)_{i \in I}$ with $\cap_{i \in I} A_i \cap X = \emptyset$, there is $I' \subset I$ finite such that $\cap_{i' \in I'} A_{i'} \cap X = \emptyset$.

A non-empty set X satisfying the conditions (i), (ii) above is called a compact set.

Ex. Prove that conditions (i), (ii) above are in fact equivalent.

Theorem 7.24 (Heine–Borel Theorem). *One has the following* **characterization** *of the compact sets. For a non-empty subset $X \subset \mathbb{R}$ the following are equivalent*

(i) *X is compact.*

(ii) *X is bounded and closed.*

(iii) *Every sequence $(x_n)_n$ with $x_n \in X$ has a convergent subsequence $x_{n_k} \to x \in X$.*

Proof. To 1): We will prove: (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i).

(i) $\Rightarrow$ (ii): We first prove that X is bounded. Let namely $U_n := (-n, n)$ for $n \in \mathbb{N}$. Then $\mathbb{R} = \cup_n U_n$ (WHY), hence $(U_n)_{n\in\mathbb{N}}$ is an open covering of X (WHY). Since X has a finite covering property, there is $n_X \in \mathbb{N}$ s.t. $X \subset (-n_X, n_X)$ (WHY), thus X is bounded (WHY). Second we prove that X is closed, or equivalently, that $X = \overline{X}$. Let $x \in \overline{X}$ be given, and by contradiction, suppose that $x \notin X$. Let $I = \mathbb{R}_{>0}$, and for $\epsilon \in I$, let $U_\epsilon := (-\infty, -\epsilon + x) \cup (x + \epsilon, \infty)$. Then $\cup_{\epsilon\in I} U_\epsilon = (-\infty, x) \cup (x, \infty)$ (WHY). Hence $x \notin X$ implies that $(U_\epsilon)_{\epsilon>0}$ is an open covering of X. Since X is compact, there is a finite set $I' \subset I$ such that $(U_\epsilon)_{\epsilon\in I'}$ is a finite covering of X. OTOH, if $\epsilon'' < \epsilon'$ then $U_{\epsilon'} \subset U_{\epsilon''}$ (WHY), thus for $\epsilon_0 := \min(I')$, one has $\cup_{\epsilon\in I'} = U_{\epsilon_0}$ (WHY), hence $X \subset U_{\epsilon_0} = (-\infty, -\epsilon_0 + x) \cup (x + \epsilon_0, \infty)$. Thus $\epsilon < \epsilon_0 \Rightarrow B_\epsilon(x) \cap X = \emptyset$ (WHY), and $x \notin \overline{X}$ (WHY), Ctr!!!

(ii) $\Rightarrow$ (iii) Let $(x_n)_n$ be a sequence with $x_n \in X$. We construct a Cauchy subsequence $(x_{n_k})_k$ of $(x_n)_n$ inductively as follows. Set $a_0 := \inf(X), b_0 = \sup(X)$, which exist in $\mathbb{R}$ (WHY), $c_0 := \frac{1}{2}(a_0 + b_0)$, and further, $N_0 := \mathbb{N}$, and $n_0 := 0$. Let $N_1' := \{n \in \mathbb{N} \,|\, x_n \in [a_0, c_0]$ and $N_1'' := \{n \in \mathbb{N} \,|\, x_n \in [c_0, b_0]\}$. Then $N_1' \cup N_1'' = N_0$, hence at least one of the sets N_1', N_1'' is infinite. First, if N_1' is infinite, set $a_1 := a_0$, $b_1 = c_0$, $c_1 := \frac{1}{2}(a_1 + b_1)$, and $N_1 = N_1'$. Second, if N_1' is finite (hence N_1'' is infinite), set $a_1 := c_0$, $b_1 = b_0$, $c_1 := \frac{1}{2}(a_1 + b_1)$, and $N_1 = N_1''$; finally set $n_1 := \min(N_1)$. Repeating inductively the steps above, suppose that $a_0 \leqslant \cdots \leqslant a_k$, $b_k \leqslant \cdots \leqslant b_0$ with $b_i - a_i = \frac{1}{2^i}(b_0 - a_0)$, and $N_i := \{n \in \mathbb{N} \,|\, x_n \in [a_i, b_i]\}$ infinite; and set $n_k = \min(N_k)$. One gets a subsequence $(x_{n_k})_k$ of $(x_n)_n$ such that $a_k \leqslant x_{n_k} \leqslant b_k$ (WHY). Since $(a_k)_k \nearrow$, $(b_k)_k \searrow$, and $b_k - a_k = \frac{1}{2^k} \to 0$, one has that $(x_{n_k})_k$ is Cauchy (WHY). Hence if $x_{n_k} \to x$ in $\mathbb{R}$, taking into account that $X = \overline{X}$ is closed, it follows by Proposition 7.19, 2) that $x \in X$.

(iii) $\Rightarrow$ (ii) By contradiction, suppose that X is not bounded, say, not bounded above. Construct sequences $(n_k)_k$ and $(x_k)_k$ such that $n_0 + 1 < x_0 < n_1 + 1 < x_2 < n_1 + 1 < \ldots$ with $x_k \in X$ (HOW). Then $|x_{k+1} - x_k| \geq 1$, hence $(x_k)_k$ cannot have a convergent subsequence (WHY). Second, we prove the X is closed. Equivalently, by Proposition 7.19, 2), we have to show: If $x_n \to x$ with $x_n \in X$, then $x \in X$ (WHY). OTOH, by the hypothesis (iii), the sequence $(x_n)_n$ has convergent subsequence $(x_{n_k})_k$ s.t. $x_{n_k} \to x' \in X$. Since $x_n \to x$, it follows that $x_{n_k} \to x$, and therefore $x = x'$ (WHY). Hence we conclude that $x \in X$.

(ii) $\Rightarrow$ (i): Since X is bounded and closed, one has $a := \inf(X)$, $b := \sup(X) \in X$ (WHY), and setting $X_x := X \cap [a, x]$ for each $x \in [a, b]$ one has: $X_a = [a, a] = \{a\}$ (WHY), $X_b = X$ (WHY), and $(U_i)_i$ is an open covering of X_x for each $x \in [a, b]$ (WHY). Consider $Y := \{x \in [a, b] \,\big|\, \text{there is a finite subcovering of } X_x\}$. Since $a \in Y$ (WHY), it follows that Y is non-empty, and obviously, b is an upper bound for Y. Hence by the Completeness Axiom, $c := \sup(Y)$ exists, and $a \leqslant c \leqslant b$ (WHY). By contradiction, suppose that $c < b$.

Case 1. $c \in X$. Then there is U_{i_c} such that $a \in U_{i_c}$, hence $\exists\, \epsilon > 0$ s.t. $B_\epsilon(c) \subset U_{i_c}$. Hence the points x, x' with $-\epsilon + c < x < c < x' < c + \epsilon$ lie in U_i, and further: First, $x \in Y$, hence $X_x = [a, x]$ has a finite subcovering $(U_i)_{i\in I'}$. Second, $X_{x'} \subset X_x \cup [x, x'] \subset \left(\cup_{i\in I'} U_i\right) \cup U_{i_c}$ (WHY). And since I' is finite, so is $I' \cup \{i_c\}$, thus $x' \in Y$. OTOH, $c = \sup(Y)$ and $c < x' \in Y$, Ctr!!!

Case 2. $c \notin X$. Since X is closed and $c \notin X$, there is $\epsilon > 0$ s.t. $X \cap B_\epsilon(c) = \emptyset$. But then all x with $-\epsilon + c < x < c$ satisfy $x \notin X$, hence $x \notin Y$, contradicting that $\sup(Y) = c$ (WHY). □

Proposition 7.25 (Compact Sets). *The compact sets have the following properties:*

1) *If X is compact, and $Y \subset X$ is a non-empty and closed, then Y is compact.*

2) *A finite union $X = \cup_\alpha X_\alpha$ of compact sets X_α is compact.*

3) *Let X_i, $i \in I$, be compact sets. Then $\cap_{i\in I} X_i = \emptyset$ iff $\exists\, I' \subset I$ finite s.t. $\cap_{i'\in I'} X_{i'} = \emptyset$.*

Proof. To 1): 1st Method: Apply the Heine-Borel Thm (**Ex** ...). 2nd Method (using definitions): $U := \complement_{\mathbb{R}}(Y)$ is open (WHY), and if $(U_i)_{i\in I}$ is an open covering of Y, then $\big(U, (U_i)_i\big)$ is an open covering of X (WHY), etc.

To 2): Let $(U_i)_{i\in I}$ be an open covering of X. Then $(U_i)_i$ is an open covering of $X_\alpha\ \forall\, \alpha$ (WHY). If $I_\alpha \subset I$ is finite s.t. $X_\alpha \subset \cup_{i\in I_\alpha} U_i$, and $I' := \cup_\alpha I_\alpha$, one has: $I' \subset I$ is finite (WHY), and $X_\alpha \subset \cup_{i\in I_\alpha} U_i \subset \cup_{i\in I'} U_i$ (WHY). Therefore, $X = \cup_\alpha X_\alpha \subset \cup_{i\in I'} U_i$. Thus $I' \subset I$ defines a finite subcovering $(U_i)_{i\in I'}$ of $(U_i)_i$ of X.

To 3): Let X_{i_0} be fixed, and replace each X_i by $X_i' := X_{i_0} \cap X_i$ (in particular, $X_{i_0}' = X_{i_0}$). Then $\cap_i X = \emptyset$ iff $\cap_i X_i' = \emptyset$ (WHY), hence w.l.o.g., we can suppose that all X_i, $i \in I$ are subsets of a fixed compact set X. Further, each X_i is closed by the Heine–Borel Thm 7.24, (ii). Hence all $U_i := \complement_{\mathbb{R}}(X_i)$ are open (WHY), and obviously, $X_i = \complement_{\mathbb{R}}(U_i)$ (WHY). For the implication " $\Rightarrow$ " one has: $\cap_i X_i = \emptyset$ iff $\complement_{\mathbb{R}}(\cap_i X_i) = \mathbb{R}$ iff $\cup_i U_i = \mathbb{R}$ (WHY). Hence $\cap_i X_i = \emptyset$ implies $X \subset \cup_i U_i$, i.e., $(U_i)_i$ is an open covering of X (WHY). Since X is compact, $\exists\, I' \subset I$ finite s.t. $(U_i)_{i\in I'}$ is a finite subcovering of $(U_i)_i$ for X, i.e., $X \subset \cup_{i\in I'} U_i$. Since $X \subset \cup_{i\in I'} U_i$, one has $X \cap \big(\complement_{\mathbb{R}}(\cup_{i\in I'} U_i)\big) = \emptyset$ (WHY). OTOH, $\complement_{\mathbb{R}}(\cup_{i\in I'} U_i)\big) = \cap_{i\in I'} X_i$ (WHY), concluding that $X \cap \big(\cap_{i\in I'} X_i\big) = \emptyset$, thus $\cap_{i\in I'} X_i = \emptyset$ because $X_i \subset X$ for all $i \in I$. The converse implication is clear **Ex** ... □

8. The Field of Complex Numbers $\mathbb{C}, +, \cdot, \leqslant$

A drawback of the field of real numbers is the fact that there are simple algebraic equations like $x^2 + 1 = 0$ which have no solution in $\mathbb{R}$. The remedy for that is to introduce a bigger domain of numbers in which *all polynomial equations in one variable,* i.e., of the form $a_n x^n + \cdots + a_1 x + a_0 = 0$, $a_n \neq 0$, have solutions. Such a domain of numbers exists, namely

field of complex numbers $\mathbb{C}, +, \cdot$.

In particular, if $\boldsymbol{i}$ is a solution of $x^2 + 1_{\mathbb{C}} = 0$, then $\boldsymbol{i}^2 = -1_{\mathbb{C}}$ (WHY). Hence by the properties of totally ordered rings/fields, it follows that $\mathbb{C}$ **cannot** carry a total ordering compatible with addition and multiplication (WHY).

... to be continued ...

9. Topological/metric Spaces/Continuity

9.1 Topological/metric spaces

9.2 Connectedness/Compactness

9.3 Continuos maps/Properties

9.4 Elementary functions/Analytic functions

10. Differentiability

10.1 Definitions/Properties

10.2 Rolle & Lagrange Thms/Consequences

10.3 Elementary Functions/Analytic functions

11. Antiderivates / Arc length / Area

11.1 Antiderivates / Basic properties

11.2 Riemann sums / Existence of antiderivatives

11.3 Arc Length / Applications

11.4 Area / Applications

E-mail address: pop@math.upenn.edu
URL: http://math.penn.edu/~pop