4. CARDINALITY (cf. Ch. 8)

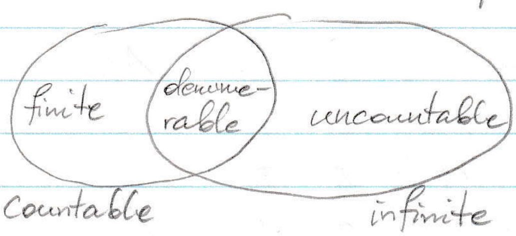
Def. Two sets A, B are <u>equinumerous</u> (or <u>have the same cardinality</u>), when $\exists$ bijection $f: A \leftrightarrow B$. We write $A \sim B$, or $|A| = |B|$.

Remark + Def. Note that $A \sim A$, $A \sim B \Rightarrow B \sim A$, and $A \sim B \wedge B \sim C \Rightarrow A \sim C$, so $\sim$ is an equivalence relation on sets.
Its equivalence classes are called <u>cardinal numbers</u>. The class of A is denoted by $|A|$.

Def. A set X is <u>finite</u>, when $X = \emptyset$ or $\exists n \in \mathbb{N}_+$ $\exists$ bijection $f: \{1, \dots, n\} \leftrightarrow X$.
Otherwise, X is called <u>infinite</u>.

Notation: $\{1, \dots, n\} =: I_n$. (Thus, X finite iff $X = \emptyset$ or $|X| = |I_n|$ for some $n \in \mathbb{N}_+$)

Def.
- For $n \in \mathbb{N}_+$, we identify $|I_n|$ with n.
- If a set X satisfies $X \sim I_n$, we say that <u>X has n elements</u> and write $|X| = n$.
- $|\emptyset| := 0$.
- If $|X| \neq n$, $\forall n \in \mathbb{N}$, then the cardinal number of X is called <u>transfinite</u>.
- X is called <u>denumerable</u>, when $\exists$ bijection $f: \mathbb{N}_+ \leftrightarrow X$.



- A finite or denumerable set is called <u>countable</u>. All other sets are <u>uncountable</u>.

<u>Countable Sets</u>

$$|\mathbb{N}| = \aleph_0 = \text{aleph naught}$$

<u>Examples</u>: 1) $\mathbb{N} \sim 2\mathbb{N}$: $f(n) = 2n$, $\forall n \in \mathbb{N}$

2) $\mathbb{N} \sim \mathbb{Z}$: $f(n) = \begin{cases} k, & \text{if } n = 2k \\ -k, & \text{if } n = 2k-1. \end{cases}$

$$\begin{array}{cccccccccc} \mathbb{N}: & 0 & 1 & 2 & 3 & 4 & 5 & 6 & \dots \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \\ \mathbb{Z}: & 0 & -1 & 1 & -2 & 2 & -3 & 3 & \dots \end{array}$$

Thm. Let A be a set. Then,
A is infinite iff $\exists B \subsetneq A$ s.t. $\exists$ bijection $f: B \twoheadrightarrow A$.

Proof = Exercise.

Thm. Let A be a countable set, and let $B \subset A$. Then, B is countable.

Pf: If B is finite, we're done. Suppose then that $|B| \neq n$, $\forall n \in \mathbb{N}$.
Then also $|A| \neq n$, $\forall n \in \mathbb{N}$ (since $B \subset A$), so we may fix a bijection $f: \mathbb{N}_+ \twoheadrightarrow A$.
We may thus write $A = \{a_1, a_2, a_3, \ldots\}$, where $a_n = f(n)$.
Set $X := f^{-1}(B)$. By assumption $B \neq \phi$, and thus $X \neq \phi$. By the well-ordering property of $\mathbb{N}$, X has a unique minimal element, say n_1.
Define a function $g: \mathbb{N}_+ \to X$ recursively by setting $g(1) := n_1$, and for $k \geq 1$,
$g(k+1) = n_k := \min\{\ell \in \mathbb{N} \mid \ell \in X \setminus \{g(1), \ldots, g(k)\}\}$.
By definition, $\forall k$, $g(k+1) > g(k) \geq k$, so g is injective. Note that, $\forall k$, $g(k)$ is well-defined, as $X \setminus \{g(1), \ldots, g(k-1)\} \neq \phi$ (for else B would be finite).
It follows that $f \circ g: \mathbb{N}_+ \to B$ is an injection, and by construction it is also surjective. Thus, $f \circ g: \mathbb{N}_+ \twoheadrightarrow B$ is bijective, which proves that B is denumerable. ∎

Thm. Let A be a nonempty set. TFAE:
(i) A is countable
(ii) There is an injection $f: A \hookrightarrow \mathbb{N}_+$.
(iii) There is a surjection $g: \mathbb{N}_+ \twoheadrightarrow A$.

Pf:
(i) $\Rightarrow$ (ii): Suppose A is countable. Then, by definition, $\exists n \in \mathbb{N}_+$ $\exists$ bijection $h_1: A \twoheadrightarrow I_n$ or else $\exists$ bijection $h_2: \mathbb{N}_+ \twoheadrightarrow A$.
In the first case, set $f := \imath \circ h_1$, where $\imath: I_n \hookrightarrow \mathbb{N}_+$ is the inclusion.
In the second case, set $f := h_2^{-1}$. ✓

(ii) $\Rightarrow$ (iii): Let $f: A \hookrightarrow \mathbb{N}_+$ be given. Then, $f: A \twoheadrightarrow f(A)$ is a bijection, so f^{-1} is a bijection from $f(A) \subseteq \mathbb{N}$ onto A. Pick $a_0 \in A$, and define

$$g(n) := \begin{cases} f^{-1}(n), & \text{if } n \in f(A) \\ a_0, & \text{otherwise.} \end{cases}$$

✓

(iii) $\Rightarrow$ (i): Let $g: \mathbb{N}_+ \twoheadrightarrow A$ be given. Define $h: A \to \mathbb{N}_+$ by
$$h(a) := \min\{n \in \mathbb{N}_+ \mid g(n) = a\}.$$
Then, h is injective ($a_1 \neq a_2 \Rightarrow \nexists\, n \in \mathbb{N}_+$ s.t. $g(n) = a_1 \wedge g(n) = a_2 \Rightarrow h(a_1) \neq h(a_2)$), and so h is a bijection from A onto $h(A) \subseteq \mathbb{N}_+$. By the previous theorem, $h(A)$ is countable, and hence so is A, as $A \sim h(A)$. ∎

<u>More Examples of Countable Sets:</u>

1) S, T countable $\Rightarrow S \cup T$ countable.

Pf: W.l.o.g. assume $S \neq \emptyset \neq T$. Then, by above thm., there are surjections $f: \mathbb{N}_+ \twoheadrightarrow S$, $g: \mathbb{N}_+ \twoheadrightarrow T$.
Define
$$h: \mathbb{N}_+ \ni n \longmapsto \begin{cases} f\left(\frac{n+1}{2}\right), & n \text{ odd} \\ g\left(\frac{n}{2}\right), & n \text{ even}. \end{cases}$$
Then, h is onto $S \cup T$, because $\forall k \in \mathbb{N}_+\ \exists n \in \mathbb{N}_+$ s.t. $k = \frac{n+1}{2}$ &
$\forall k \in \mathbb{N}_+\ \exists m \in \mathbb{N}_+$ s.t. $k = \frac{m}{2}$. ∎

2) S, T countable $\Rightarrow S \times T$ countable.

Pf. If $S = \emptyset$ or $T = \emptyset$, then $S \times T = \emptyset$, so we may assume $S \neq \emptyset \neq T$.
There are injections $f: S \hookrightarrow \mathbb{N}_+$ and $g: T \hookrightarrow \mathbb{N}_+$.
Define
$$h: S \times T \ni (s,t) \longmapsto 2^{f(s)} \cdot 3^{g(t)} \in \mathbb{N}_+.$$
Then, h is injective, because $2^{f(s_1)} \cdot 3^{g(t_1)} = 2^{f(s_2)} \cdot 3^{g(t_2)} \Leftrightarrow f(s_1) - f(s_2) = 0 \wedge$
$\wedge\, g(t_2) - g(t_1) = 0$. ∎

3) $\mathbb{Q}$ is countable.

Pf. Write $\mathbb{Q} = \mathbb{Q}_- \cup \{0\} \cup \mathbb{Q}_+$. By the first example above, it suffices to show that $\mathbb{Q}_+$ is countable (as $\mathbb{Q}_- \sim \mathbb{Q}_+$ by the bijection $q \mapsto -q$). Now, for any $q \in \mathbb{Q}_+$, there is a unique pair $(m_q, n_q) \in \mathbb{N}_+ \times \mathbb{N}_+$ s.t. $(m_q, n_q) = 1$ (rel. prime) $\wedge\ q = \frac{m_q}{n_q}$. Define $f: \mathbb{Q} \to \mathbb{N}_+$ as
$$f(q) := 2^{m_q} \cdot 3^{n_q}.$$

Then, f is injective, b/c $2^{m_q}\cdot 3^{n_q} = 2^{m_p}\cdot 3^{n_p} \Rightarrow 2^{m_q-m_p} = 3^{n_p-n_q} \Rightarrow$
$\Rightarrow m_q - m_p = 0 = n_p - n_q \Rightarrow (m_q, n_q) = (m_p, n_p) \Rightarrow q = p.$ ∎

4) Countable union of countable sets is countable.

Pf. Let $\{A_n\}_{n=1}^{\infty}$ be a family of countable sets. W.l.o.g. we may assume that each A_n is denumerable. Write the elements of all the A_n in an infinite matrix:

$$\begin{array}{ll}
A_1: & a_{11},\ a_{12},\ a_{13},\ a_{14}, \ldots \\
A_2: & a_{21},\ a_{22},\ a_{23},\ a_{24}, \ldots \\
A_3: & a_{31},\ a_{32},\ a_{33},\ a_{34}, \ldots \\
A_4: & a_{41}, \ldots \\
\vdots &
\end{array}$$

this listing defines a surjection $\mathbb{N}_+ \twoheadrightarrow \bigcup_{n=1}^{\infty} A_n$.

<u>Thm.</u> (Cantor) The set $\mathbb{R}$ is not countable.

Pf. For a proof by contradiction suppose $\mathbb{R}$ is countable, and let $\{r_1, r_2, r_3, \ldots\}$ be the listing of all the elements of $\mathbb{R}$. Write the decimal expansions of the r_n in an infinite matrix:

$$\begin{array}{l}
r_1 = a_{10}.\, a_{11}\ a_{12}\ a_{13}\ a_{14}\ a_{15} \ldots \\
r_2 = a_{20}.\, a_{21}\ a_{22}\ a_{23}\ a_{24}\ a_{25} \ldots \\
r_3 = a_{30}.\, a_{31}\ a_{32}\ a_{33}\ a_{34}\ a_{35} \ldots \\
\vdots
\end{array}$$

where the $a_{i0} = \lfloor r_i \rfloor$ is the integral part of r_i, and $a_{i1}, a_{i2}, a_{i3}, \ldots \in \{0, 1, \ldots, 9\}$ are the consecutive digits of its decimal expansion.

Define $t \in \mathbb{R}$ to be the number given by a decimal expansion $b_0.\, b_1 b_2 b_3 b_4 \ldots$, where

$$b_i := \begin{cases} 5, & \text{if } a_{ii} \neq 5 \\ 0, & \text{if } a_{ii} = 5. \end{cases}$$

By construction, $\forall k \in \mathbb{N}_+$, $t \neq r_k$, because their decimal exp's disagree in the k'th place. ↯ ∎

Ordering of Cardinals

Def. We define the "$\leq$" relation on cardinal numbers by setting $|A| \leq |B|$, when there is an injection $A \hookrightarrow B$.

Thm. (Cantor–Bernstein) If $|X| \leq |Y|$ and $|Y| \leq |X|$, then $|X| = |Y|$.
That is, if there are injections $X \hookrightarrow Y$ and $Y \hookrightarrow X$, then there is a bijection $X \hookrightarrow\!\!\!\rightarrow Y$.

Pf. Given injections $f: X \hookrightarrow Y$, $g: Y \hookrightarrow X$, define $\varphi := g \circ f : X \to X$.
Then, φ is an injection and hence a bijection from X onto $\varphi(X)$.
Set $Z := g(Y)$, and $V := X \setminus Z$.
Then, $g: Y \hookrightarrow\!\!\!\rightarrow Z$, and $\varphi(X) \subseteq Z \subseteq X$. $(*)$

Notation:
Given $\varphi: X \to X$, $C \subseteq X$, set $\varphi^0(C) := C$, $\varphi^{k+1}(C) := \varphi(\varphi^k(C))$, $k \in \mathbb{N}$.

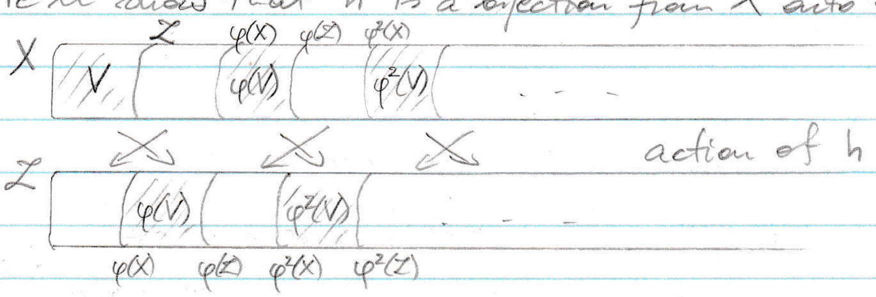
Observations:
(i) $\forall n \in \mathbb{N}$, $\varphi^{n+1}(X) \subseteq \varphi^n(Z) \subseteq \varphi^n(X)$ (from $(*)$)
(ii) $\forall n \in \mathbb{N}$, $\varphi^n(X) \setminus \varphi^n(Z) = \varphi^n(V)$ (by def. of V and inj. of φ)
(iii) $\forall n \in \mathbb{N}$, $\varphi^n(V) \cap \varphi^n(Z) = \emptyset$ (— " —)
(iv) $\forall k, l \in \mathbb{N}$, $k < l \Rightarrow \varphi^k(X) \supseteq \varphi^l(X)$ (b/c $\varphi(X) \subseteq X$)
(v) $\forall k, l \in \mathbb{N}$, $k < l \Rightarrow \varphi^k(Z) \supseteq \varphi^l(X) \supseteq \varphi^l(V)$ (by (i) & (iv))

Now, define

$$S := V \cup \varphi(V) \cup \varphi^2(V) \cup \ldots = \underbrace{\bigcup_{k \in \mathbb{N}} \varphi^k(V)}_{\text{disjoint (!) union, by (iii)+(v)}}, \text{ and}$$

$$h: X \to X \text{ by } h(x) := \begin{cases} \varphi(x), & \text{if } x \in S \\ x, & \text{if } x \in X \setminus S. \end{cases}$$

We'll show that h is a bijection from X onto Z.



a) Injectivity of h follows easily from injectivity of φ.
b) Surjectivity: $h(S) = \varphi(S) = \varphi(\bigcup_{k=0}^{\infty} \varphi^k(V)) = \bigcup_{k=0}^{\infty} \varphi^{k+1}(V) = \bigcup_{l=1}^{\infty} \varphi^l(V) = S \setminus V$,

b/c by (v), $\bigcup_{l \geq 1} \varphi^l(V) \subseteq \varphi^0(Z) = Z$ and $Z \cap V = \emptyset$.

Also, $h(X \setminus S) = X \setminus S$. Hence, $h(X) = h(S \cup (X \setminus S)) = h(S) \cup h(X \setminus S) =$

$= (S \setminus V) \cup (X \setminus S) = X \setminus V = Z$. ✓

Thus, $h: X \leftrightarrow\!\!\!\rightarrow Z$ and composing with the inverse of $g: Y \leftrightarrow\!\!\!\rightarrow Z$, we get $X \sim Y$. ∎

Thm. For any set S, we have $|S| < |\mathcal{P}(S)|$.

Pf. Clearly, $|S| \leq |\mathcal{P}(S)|$ for any S, b/c there is an injection $S \ni s \mapsto \{s\} \in \mathcal{P}(S)$. ✓

Suppose then that there is a set S st. $|S| = |\mathcal{P}(S)|$, and let $f: S \leftrightarrow\!\!\!\rightarrow \mathcal{P}(S)$ be a bijection.

Define $T := \{s \in S \mid s \notin f(s)\}$.

By bijectivity of f, $\exists!\, t \in S$ st. $T = f(t)$. Then, $t \in T \Rightarrow t \notin T$ and $t \notin T \Rightarrow \neg(t \notin T)$. ↯ ∎

Corollary. $\aleph_0 = |\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \ldots$ is an infinite sequence of cardinals.

Continuum Hypothesis (Cantor):

There's no set X s.t. $\aleph_0 < |X| < \mathfrak{c}$, where $\mathfrak{c} = |\mathcal{P}(\mathbb{N})|$.

Cardinal Arithmetic:

Def. Given cardinal numbers α, β, we define

- $\alpha + \beta := |A \cup B|$, where $|A| = \alpha$, $|B| = \beta$, and $A \cap B = \emptyset$
- $\alpha \cdot \beta := |A \times B|$, where $|A| = \alpha$, $|B| = \beta$.

Prop. The above are well-defined; i.e., independent of the choice of representatives.

Pf = Exercise.

Prop. For any cardinal numbers α, β, γ, we have:

(a) $\alpha + \beta = \beta + \alpha$

(b) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$

(c) $\alpha \cdot \beta = \beta \cdot \alpha$

(d) $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

(e) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

Pf. (e): $A \times (B \cup C) = (A \times B) \cup (A \times C)$. ✓

The other points are trivial. ∎

Notation: $\mathcal{P}(X) = 2^X$.

Justification: Every subset Y of X can be identified with its characteristic function (rel. X), $\chi_Y : X \to \{0,1\}$.

If $|X| < \aleph_0$, then $\#\{\text{characteristic functions}\} = 2^{|X|}$.

Thm. $|2^{\mathbb{N}}| = \mathfrak{c}$.

Pf. Let $\mathcal{F} = \{\chi_A \mid A \subseteq \mathbb{N}_+\}$. Define $f : \mathcal{F} \ni \chi_A \mapsto \underbrace{0.\chi_A(1)\chi_A(2)\chi_A(3)\ldots}_{\text{binary expansion}} \in [0,1]$

Then, f is surjective, and hence $\exists$ inj. $g : [0,1] \hookrightarrow \mathcal{F}$.

Since $[0,1] \sim (0,1) \sim \mathbb{R}$, and $\mathcal{F} \sim 2^{\mathbb{N}}$, it follows that:

$x \mapsto \tan(\pi x - \frac{\pi}{2})$

$$\mathfrak{c} = |[0,1]| \le |\mathcal{F}| = |2^{\mathbb{N}}|.$$

On the other hand, $\tilde{f} : \mathcal{F} \ni \chi_A \mapsto 0.\chi_A(1)\chi_A(2)\chi_A(3)\ldots$ as a decimal exp. $\in [0,1]$ is (clearly) injective, and so $|2^{\mathbb{N}}| = |\mathcal{F}| \le \mathfrak{c}$.

The result thus follows from Cantor-Bernstein. ∎

Thm. $\aleph_0$ is the least transfinite cardinal. I.e, $\forall$ cardinal α, $[\forall n \in \mathbb{N}, \alpha \ne n] \Rightarrow \aleph_0 \le \alpha$.

Pf. Axiom of choice. ∎

Prop. $|\mathbb{R} \setminus \mathbb{Q}| = |\mathbb{R}|$.

Pf. Clearly, $\mathbb{R} \setminus \mathbb{Q}$ is infinite. Hence, $|\mathbb{R} \setminus \mathbb{Q}| \ge \aleph_0$, by above.

Suppose $|\mathbb{R} \setminus \mathbb{Q}| = \aleph_0$. Then, $|\mathbb{R}| = |(\mathbb{R} \setminus \mathbb{Q}) \sqcup \mathbb{Q}| = \aleph_0 + \aleph_0 = \aleph_0$; contradiction.

Thus, $\aleph_0 < |\mathbb{R} \setminus \mathbb{Q}|$.

On the other hand, $|\mathbb{R} \setminus \mathbb{Q}| \le |\mathbb{R}|$, so the claim follows from the Continuum Hypothesis. ∎

Prop. (i) $\forall n \in \mathbb{N}$, $n + \aleph_0 = \aleph_0$.

(ii) $\forall n \in \mathbb{N}_+$, $n \cdot \aleph_0 = \aleph_0$.

(iii) $\aleph_0 \cdot \aleph_0 = \aleph_0$.

(iv) $\forall \alpha, \beta$ transfinite $\forall n \in \mathbb{N}$, $n + \alpha = \aleph_0 + \beta \iff \alpha = \beta$,

$\aleph_0 + \alpha = \aleph_0 + \beta \iff \alpha = \beta$.

Example: The Cantor set (ternary) is uncountable.

III. REAL NUMBERS (cf. Ch. 3)

1. ORDERED FIELDS

Def. A *field* is a triple $(\mathbb{F}, +, \cdot)$ where $\mathbb{F}$ is a nonempty (!) set, "$+$": $\mathbb{F}\times\mathbb{F} \to \mathbb{F}$ and "$\cdot$": $\mathbb{F}\times\mathbb{F}\to\mathbb{F}$ are functions, called *addition* and *multiplication*, satisfying the following axioms:

(A1) $\forall x,y\in\mathbb{F}$, $x+y\in\mathbb{F}$

(A2) $\forall x,y\in\mathbb{F}$, $x+y=y+x$ /commutativity/

(A3) $\forall x,y,z\in\mathbb{F}$, $x+(y+z)=(x+y)+z$ /associativity/

(A4) there exists an element $0\in\mathbb{F}$ s.t. $\forall x\in\mathbb{F}$, $x+0=x$ /additive identity/

(A5) $\forall x\in\mathbb{F}$ $\exists y\in\mathbb{F}$ s.t. $x+y=0$. We write $y=-x$. /additive inverse/

(M1) $\forall x,y\in\mathbb{F}$, $x\cdot y\in\mathbb{F}$

(M2) $\forall x,y\in\mathbb{F}$, $x\cdot y=y\cdot x$

(M3) $\forall x,y,z\in\mathbb{F}$, $x\cdot(y\cdot z)=(x\cdot y)\cdot z$

(M4) there exists an element $1\in\mathbb{F}\setminus\{0\}$ s.t. $\forall x\in\mathbb{F}$, $x\cdot 1=x$ /multiplicative identity/

(M5) $\forall x\in\mathbb{F}\setminus\{0\}$ $\exists y\in\mathbb{F}$ s.t. $x\cdot y=1$. We write $y=x^{-1}$ (or $\frac{1}{x}$)

(DL) $\forall x,y,z\in\mathbb{F}$, $x\cdot(y+z)=x\cdot y+x\cdot z$. /distributive law/

(cf. 3.4) **Thm.** Let $(\mathbb{F},+,\cdot)$ be a field. Then,

(i) The additive and multiplicative identities are unique.

(ii) $\forall x\in\mathbb{F}$, $-x$ is unique.

(iii) $\forall x\in\mathbb{F}\setminus\{0\}$, x^{-1} is unique.

(iv) $\forall x,y,z\in\mathbb{F}$, $(x+z=y+z)\Rightarrow(x=y)$ /cancelation law/

(v) $\forall x\in\mathbb{F}$, $x\cdot 0=0$

(vi) $\forall x\in\mathbb{F}$, $(-1)\cdot x=-x$

(vii) $\forall x,y\in\mathbb{F}$, $x\cdot y=0\Rightarrow(x=0 \vee y=0)$

(viii) $\forall x,y\in\mathbb{F}$ $\exists!\, z\in\mathbb{F}$ s.t. $x=y+z$ /subtraction/

(ix) $\forall x\in\mathbb{F}$ $\forall y\in\mathbb{F}\setminus\{0\}$ $\exists!\, z\in\mathbb{F}$ s.t. $x=y\cdot z$ /division/

Pf. (i) Suppose $0_1, 0_2$ both satisfy (A4). Then, $0_1 \overset{(A4)\text{ for }0_2}{=} 0_1+0_2 \overset{(A2)}{=} 0_2+0_1 \overset{(A4)\text{ for }0_1}{=} 0_2$. ✓

Similarly, if $1_1, 1_2$ both satisfy (M4), then $1_1 \underset{(M4)\text{ for }1_2}{=} 1_1\cdot 1_2 \underset{(M2)}{=} 1_2\cdot 1_1 \underset{(M4)\text{ for }1_2}{=} 1_2$. ✓

(ii) Given $x\in\mathbb{F}$, suppose $x+y=0 \wedge x+z=0$. Then, $y=y+0=y+(x+z)=(x+y)+z=0+z=z$. ✓

(iii) Given $x\in\mathbb{F}\setminus\{0\}$, suppose $x\cdot y=1 \wedge x\cdot z=1$. Then, $y=y\cdot 1=y\cdot(x\cdot z)=(x\cdot y)\cdot z=1\cdot z=z\cdot 1=z$. ✓

(iv) Let x,y,z be s.t. $x+z=y+z$. Then, $x=x+0=x+(z+(-z))=(x+z)+(-z)=y+(z+(-z))$
$=y+0=y$. ✓

(v) Given $x\in\mathbb{F}$, we have $x\cdot 0=x\cdot(0+0)=x\cdot 0+x\cdot 0$. On the other hand, $x\cdot 0=x\cdot 0+0$, hence $0+x\cdot 0=x\cdot 0+x\cdot 0$, and thus $0=x\cdot 0$, by (iv). ✓

(vi) Given $x\in\mathbb{F}$, $(-1)\cdot x+x=((-1)+1)\cdot x=0\cdot x=0$, by (v). By (ii) then, $(-1)\cdot x=-x$. ✓

(vii) Suppose $x,y\in\mathbb{F}\setminus\{0\}$ and $x\cdot y=0$. Then, both x and y have multiplicative inverses and hence $1=\underset{\text{by (M4)},\ 1\neq 0}{1\cdot 1}=x^{-1}\cdot x\cdot y\cdot y^{-1}=x^{-1}\cdot 0\cdot y^{-1}=x^{-1}\cdot 0=0$, by (v). This contradicts (M4). ✓

(viii) Given $x,y\in\mathbb{F}$, define $z=x+(-y)$. Then, $x=x+0=x+(y+(-y))=y+(x+(-y))=y+z$. If, for some other $w\in\mathbb{F}$, $x=y+w$, then $y+w=y+z \overset{(iv)}{\Longrightarrow} w=z$. ✓

(ix) Given $x\in\mathbb{F}$ and $y\in\mathbb{F}\setminus\{0\}$, define $z=x\cdot(y^{-1})$. Then $x=x\cdot 1=x\cdot(y\cdot y^{-1})=y\cdot(x\cdot y^{-1})=y\cdot z$. If also $x=y\cdot w$, then $w=1\cdot w=y^{-1}\cdot yw=y^{-1}x=y^{-1}\cdot y\cdot z=1\cdot z=z$. ∎

Def. The characteristic of a field $\mathbb{F}$ is defined as

$$\mathrm{char}(\mathbb{F})=\begin{cases} p, & \text{if } p=\min\{k\in\mathbb{N} \mid \overbrace{1+1+\ldots+1}^{k \text{ times}}=0\} \\ 0, & \text{if there's no such } p \end{cases}$$

Examples:

1) $\mathbb{Q}=\{p/q : p\in\mathbb{Z}, q\in\mathbb{N}_+\}$ = rational numbers – the smallest field of characteristic 0.

2) $\mathbb{R}$, $\mathbb{C}$ – other fields of characteristic 0

3) If $p\in\mathbb{N}$ is a prime, define $\mathbb{Z}_p:=\{\bar{0},\bar{1},\bar{2},\ldots,\overline{p-1}\}$ with addition and multiplication induced from $\mathbb{Z}$ modulo p (i.e. $\bar{m}+\bar{n}:=\overline{m+n}$, $\bar{m}\cdot\bar{n}:=\overline{mn}$). Then, $\mathbb{Z}_p$ is a field and $\mathrm{char}(\mathbb{Z}_p)=p$.

Def. An ordered field is a field equipped with a linear order relation compatible with the field addition and multiplication. That is, $(\mathbb{F},+,\cdot)$ is an ordered field, when there is a relation "$<$" on $\mathbb{F}$ satisfying the following

(O1) $\forall x,y\in\mathbb{F},\ x<y \vee x=y \vee y<x$ /trichotomy/

(O2) $\forall x,y,z\in\mathbb{F},\ x<y \wedge y<z \Rightarrow x<z$ /transitivity/

(O3) $\forall x,y,z\in\mathbb{F},\ x<y \Rightarrow x+z<y+z$

(O4) $\forall x,y,z\in\mathbb{F},\ x<y \wedge 0<z \Rightarrow x\cdot z<y\cdot z$

Notation: We write $x\leq y$, when $x<y \vee x=y$.

Examples: $\mathbb{Q}$, $\mathbb{R}$ with usual $<$. But, $\mathbb{C}$ or $\mathbb{Z}_p$ are not ordered fields!

Def. Let $(\mathbb{F},<)$ be an ordered field. We say that an element $a\in\mathbb{F}$ is positive when $0<a$, and negative when $a<0$. (Also, nonnegative when $0\le a$.)

(cf. 3.5) **Thm.** Let $(\mathbb{F},<)$ be an ordered field, $x,y,z,w\in\mathbb{F}$. Then,

(i) $(x<y \wedge z<w) \Rightarrow x+z<y+w$.

(ii) $x<y \Rightarrow -y<-x$.

(iii) $(x<y \wedge z<0) \Rightarrow x\cdot z > y\cdot z$

(iv) $0<1$.

(v) $x>0 \Rightarrow 1/x>0$.

(vi) $0<x<y \Rightarrow 1/x > 1/y$.

Pf. (i) Suppose $x<y \wedge z<w$. Then, $x+z \overset{(O3)}{<} y+z = z+y \overset{(O3)}{<} w+y = y+w$. ✓

(ii) Suppose $x<y$. Then, $-y = -y+0 = -y+(x+(-x)) = x+(-y+(-x)) < (y+(-y))+(-x) =$
$= 0+(-x) = -x$. ✓

(iii) By (ii), if $z<0$, then $-z>-0$. But $-0=0$, so $0<-z$. Then,
$x<y \overset{(O4)}{\Rightarrow} x\cdot(-z) < y\cdot(-z) \Rightarrow -xz < -yz \overset{(ii)}{\Rightarrow} -(-yz) < -(-xz) \Rightarrow yz < xz$. ✓
by uniqueness of additive inverse

(iv) By definition $0\neq 1$. Suppose then that $1<0$.
Then, $1 = 1\cdot 1 \overset{(iii)}{>} 1\cdot 0 = 0$ which contradicts $1<0$. Thus, by (O1), $0<1$. ✓

(v) Suppose $x>0$. Then, $\neg(\frac{1}{x}=0)$, for else $1 = x\cdot\frac{1}{x} = x\cdot 0 = 0$; a contradiction.
By (O1) thus $\frac{1}{x}<0$ or $\frac{1}{x}>0$. Suppose $\frac{1}{x}<0$. Then, by (iii),
$x>0 \Rightarrow 1 = x\cdot\frac{1}{x} < 0\cdot\frac{1}{x} = 0$, which contradicts (iv). Thus, $\frac{1}{x}>0$. ✓

(vi) Suppose $0<x<y$. Then, $\neg(\frac{1}{x}=\frac{1}{y})$, for else $1 = x\cdot\frac{1}{x} = x\cdot\frac{1}{y} \underset{\text{by (O4) \& (v)}}{<} y\cdot\frac{1}{y} = 1$; a contradiction
Thus, by (O1), $\frac{1}{x}<\frac{1}{y}$ or $\frac{1}{y}<\frac{1}{x}$
Suppose $\frac{1}{x}<\frac{1}{y}$. Then, $1 = x\cdot\frac{1}{x} < x\cdot\frac{1}{y} < y\cdot\frac{1}{y} = 1$; a contradiction. Thus, $\frac{1}{y}<\frac{1}{x}$. ∎

Thm. Let $(\mathbb{F},<)$ be an ordered field. Then, there is an injection $\mathbb{N}\xrightarrow{\varphi}\mathbb{F}$, such that elements of $\varphi(\mathbb{N}_+)$ are positive, and $\mathrm{char}(\mathbb{F})=0$.

Pf. Define a function $\varphi:\mathbb{N}\to\mathbb{F}$ recursively by $\varphi(0_{\mathbb{N}}):=0_{\mathbb{F}}$, $\varphi(n+1_{\mathbb{N}}):=\varphi(n_{\mathbb{N}})+1_{\mathbb{F}}$ for all $n\in\mathbb{N}_+$. Then, by above thm., $\forall n\in\mathbb{N}$, $\varphi(n)=0+\varphi(n)<1+\varphi(n)=\varphi(n+1)=0+\varphi(n+1)<$
$<1+\varphi(n+1)=\varphi(n+2)<\ldots$ One easily proves by induction that $\varphi(n)<\varphi(n+k)$, $\forall k\in\mathbb{N}_+$
Thus, φ is injective. In particular, there is no $n\in\mathbb{N}_+$ with $\varphi(n)=0$, hence $\mathrm{char}(\mathbb{F})=0$, by definition. ∎

Corollary. Every ordered field $\mathbb{F}$ contains the field of rational numbers $\mathbb{Q}$.

Pf. Let $(\mathbb{F},<)$ be an ordered field. Then, $\mathbb{N}\subset\mathbb{F}$ and hence, $\forall n\in\mathbb{N}_+$, $\frac{1}{n}\in\mathbb{F}$ (by (M5)).
Similarly, by (A5), $\forall n\in\mathbb{N}$, $-n\in\mathbb{F}$. Thus, by (M1), $\forall m,n\in\mathbb{N}_+$, $\frac{m}{n}, -\frac{m}{n}\in\mathbb{F}$. ∎

Corollary. Let $(\mathbb{F},<)$ be an ordered field, $x,y\in\mathbb{F}$.
If $\forall\varepsilon>0$, $x\leq y+\varepsilon$, then $x\leq y$.

Pf. Suppose $\forall\varepsilon>0$, $x\leq y+\varepsilon$ and $y<x$. Then $x-y>0$, and so $\varepsilon:=\frac{1}{2}\cdot(x-y)>0$.
Now, $y+\varepsilon=y+\frac{1}{2}\cdot(x-y)=\frac{1}{2}\cdot2\cdot y+\frac{1}{2}\cdot(x-y)=\frac{1}{2}\cdot(2y+x-y)=\frac{1}{2}\cdot((1+1)\cdot y+x-y)=\frac{1}{2}(y+x+(y-y))$
$=\frac{1}{2}(y+x)<\frac{1}{2}\cdot(x+x)=\frac{1}{2}\cdot2\cdot x=x$; a contradiction. ∎

Def. Let $(\mathbb{F},<)$ be an ordered field. Define the absolute value function on $\mathbb{F}$ as

$$|x|:=\begin{cases} x, & \text{when } 0\leq x\\ -x, & \text{when } x<x.\end{cases}$$

Thm. Let $(\mathbb{F},<)$ be an ordered field, $x,y\in\mathbb{F}$, $a\in\mathbb{F}$, $a\geq0$. Then,
(i) $|x|\geq0$
(ii) $|x|\leq a \iff -a\leq x\leq a$
(iii) $|x\cdot y|=|x|\cdot|y|$
(iv) $|x+y|\leq|x|+|y|$ /triangle inequality/

Pf. (i) By definition, and since $x>0\Rightarrow -x=x\cdot(-1)<0$. ✓
(ii) Suppose $|x|\leq a$. If $x\geq0$, then $x=|x|\leq a$. Also, $a\geq0\Rightarrow -a\leq0$, so $-a\leq0\leq x$. ✓
If $x<0$, then $x=-|x|=(-1)\cdot|x|\geq(-1)\cdot a=-a$. Also, $a\geq0\Rightarrow x<0\leq a$. ✓
Conversely, suppose $-a\leq x\leq a$. If $x\geq0$, then $|x|=x\leq a$. ✓
If $x<0$, then $|x|=-x$, and $-x=(-1)\cdot x\leq(-1)\cdot(-a)=a$. ✓
(iii) Exercise.
(iv) We have, by (ii), $-|x|\leq x\leq|x| \wedge -|y|\leq y\leq|y|$, hence
$-(|x|+|y|)=-|x|+(-|y|)\leq x+y\leq|x|+|y|$, hence $|x+y|\leq|x|+|y|$, by (ii) again. ∎

Def. (Interval) Let $(X,<)$ be a nonempty set with a linear order relation $<$.
A subset $I\subset X$ is called an interval (in X), when

$$\forall x,y,z\in X,\ (x\in I\wedge y\in I\wedge x<z\wedge z<y)\Rightarrow z\in I.$$

2. COMPLETENESS AXIOM

Def. Let $(X,<)$ be a nonempty set with linear ordering $<$, let $S\subset X$.

1) Element $a\in X$ is called a lower bound for S, when $a\leq s$, $\forall s\in S$.
2) If S has a lower bound, we say S is bounded below.
3) Element $a\in X$ is called an upper bound for S, when $s\leq a$, $\forall s\in S$.
4) If S has an upper bound, we say S is bounded above.
5) Element $a\in X$ is called the minimal element of S (or minimum of S), when
$$a\in S \wedge (\forall s\in S,\ a\leq s).$$
6) Element $a\in X$ is called the maximal element of S (or maximum of S), when $$a\in S \wedge (\forall s\in S,\ s\leq a).$$

Examples: Closed vs open intervals, $\mathbb{N}$, $\{\frac{1}{n} : n\in\mathbb{N}_+\}$.

Def. Let $(X,<)$ be a nonempty set w/ linear order $<$, let $S\subset X$, $S\neq\emptyset$ be bounded.

1) Element $\alpha\in X$ is called the infimum (or greatest lower bound) of S, when
$$(\forall s\in S,\ \alpha\leq s)\wedge[\forall\beta\in X,\ \alpha<\beta \Rightarrow (\exists s\in S \text{ s.t. } s<\beta)].$$
2) Element $\alpha\in X$ is called the supremum (or least upper bound) of S, when
$$(\forall s\in S,\ s\leq\alpha)\wedge[\beta\in X,\ \beta<\alpha \Rightarrow (\exists s\in S \text{ s.t. } \beta<s)].$$

Examples: $\{\frac{1}{n} : n\in\mathbb{N}_+\}$; $[0,\sqrt{2}]\cap\mathbb{Q}$ in $X=\mathbb{Q}$; $[0,\sqrt{2})$ in $\mathbb{R}$; if $\max S$ exists, then $\sup S = \max S$. (!)

Def. We say that a nonempty linearly ordered set $(X,<)$ satisfies Completeness Axiom, when every nonempty bounded above subset of X has a least upper bound.

(!) **Def.** The field $\mathbb{R}$ of real numbers is defined as the smallest (w/r/to inclusion) ordered field satisfying the Completeness Axiom.

Archimedean Property of $\mathbb{R}$

Thm. The set $\mathbb{N}$ is not bounded above in $\mathbb{R}$.

Pf. Suppose otherwise, and let $\alpha=\sup\mathbb{N}$. Then, $\alpha-1$ is not an upper bound for $\mathbb{N}$, so $\exists n_0\in\mathbb{N}$ st. $\alpha-1<n_0$. But then $\alpha<n_0+1$. ↯ ∎

Thm. TFCAE:

(i) $\mathbb{N}$ is not bounded above.

(ii) $\forall x \in \mathbb{R}\ \exists n \in \mathbb{N}$ s.t. $x < n$.

(iii) $\forall x, y \in \mathbb{R},\ x > 0 \Rightarrow \exists n \in \mathbb{N}$ s.t. $n \cdot x > y$

(iv) $\forall x \in \mathbb{R},\ x > 0 \Rightarrow \exists n \in \mathbb{N}$ s.t. $0 < \frac{1}{n} < x$.

Pf. (i) $\Rightarrow$ (ii) ✓

(ii) $\Rightarrow$ (iii): Let $x \in \mathbb{R}_+$, $y \in \mathbb{R}$ be arbitrary. By (ii), $\exists n_0 \in \mathbb{N}$ s.t. $y/x < n_0$.
Then, as $x > 0$, $y/x \cdot x < n_0 \cdot x$. ✓

(iii) $\Rightarrow$ (iv): Let $x \in \mathbb{R}_+$ be arbitrary. By (iii), $\exists n_0 \in \mathbb{N}_+$ s.t. $n_0 x > 1$.
Then, $n_0 > 0 \Rightarrow \frac{1}{n_0} > 0 \Rightarrow n_0 \cdot x \cdot \frac{1}{n_0} > 1 \cdot \frac{1}{n_0}$; i.e., $x > \frac{1}{n_0}$. ✓

(iv) $\Rightarrow$ (i): Suppose $\alpha \in \mathbb{R}$ is s.t. $\alpha \geq n,\ \forall n \in \mathbb{N}$. Then, $\alpha \geq 1 > 0$, and for all $n \in \mathbb{N}_+$, $\frac{1}{n} \leq \frac{1}{\alpha}$, contradicting (iv). ∎

Thm. For every $s \in \mathbb{R}$, $s > 0 \Rightarrow \exists x \in \mathbb{R}$ s.t. $x^2 = s$.

Pf. Given $s \in \mathbb{R}_+$, let $S := \{x \in \mathbb{R} \mid x \geq 0 \wedge x^2 < s\}$.
Then, $S \neq \emptyset$ as $0 \in S$, and S is bdd above (indeed,
$s > 0 \Rightarrow s+1 > 1 \Rightarrow (s+1)^2 > s+1 \Rightarrow s+1 \notin S$).
Let $\alpha := \sup S$. We claim that $\alpha^2 = s$. Proof by contradiction:

I. Suppose $\alpha^2 < s$.
Then, $s - \alpha^2 > 0$, so $\exists n_1 \in \mathbb{N}$ s.t. $s - \alpha^2 > \frac{1}{n_1}$, or $\alpha^2 + \frac{1}{n_1} < s$.
Now, if we find $n_2 \in \mathbb{N}$ s.t. $(\alpha + \frac{1}{n_2})^2 \leq \alpha^2 + \frac{1}{n_1}$, then $\alpha + \frac{1}{n_2} \in S$, contradicting definition of α.
So, it suffices to find $n_2 \in \mathbb{N}_+$ s.t. $\alpha^2 + \frac{2\alpha}{n_2} + \frac{1}{n_2^2} \leq \alpha^2 + \frac{1}{n_1}$, or $\frac{2\alpha}{n_2} + \frac{1}{n_2^2} \leq \frac{1}{n_1}$.
Since $1 \leq n_2$ then $\frac{2\alpha}{n_2} + \frac{1}{n_2^2} \leq \frac{2\alpha + 1}{n_2}$. Choosing $n_2 \geq n_1 (2\alpha + 1)$ does the job. ✓

II. Suppose then that $s < \alpha^2$.
Then, $\exists n_1 \in \mathbb{N}_+$ s.t. $\alpha^2 - s > \frac{1}{n_1}$, or $\alpha^2 - \frac{1}{n_1} > s$.
Again, we look for $n_2 \in \mathbb{N}_2$ s.t. $(\alpha - \frac{1}{n_2})^2 \geq \alpha^2 - \frac{1}{n_1}$, b/c for such n_2 we get that $\alpha - \frac{1}{n_2} \notin S$ and hence $\sup S \leq \alpha - \frac{1}{n_2}$, contradicting definition of α.
Need $\alpha^2 - \frac{2\alpha}{n_2} + \frac{1}{n_2^2} \geq \alpha^2 - \frac{1}{n_1}$, or $\frac{1}{n_1} \geq \frac{2\alpha}{n_2} - \frac{1}{n_2^2}$.
Now, if $1/n_1 \geq \frac{2\alpha}{n_2}$, then also $1/n_1 \geq 2\alpha/n_2 - 1/n_2^2$, so suffices to have
$n_2 \geq n_1 \cdot 2\alpha$. ∎

Corollary. For every prime number p, there exists $x_p \in \mathbb{R}$ s.t. $x_p^2 = p$. Hence, $\mathbb{Q} \subsetneq \mathbb{R}$.

Density of $\mathbb{Q}$ in $\mathbb{R}$

Thm. If $x, y \in \mathbb{R}$, $x<y$, then there is $q \in \mathbb{Q}$ s.t. $x < q < y$.

Pf. By Archimedean Principle, $y>x \Rightarrow y-x>0 \Rightarrow \exists n \in \mathbb{N}$ s.t. $\frac{1}{n} < \frac{y-x}{2}$. Fix such n_0. Then, $\exists k_0 \in \mathbb{N}$ s.t. $x < \frac{k_0}{n_0} < y$. Indeed, $\exists k \in \mathbb{N}$ s.t. $k > n_0 \cdot x$. Let k_0 be the minimal such k (exists, by Well-ordering Principle). Then, $k_0 - 1 \le n_0 \cdot x$, so $\frac{k_0}{n_0} \le x + \frac{1}{n_0} < x + \frac{y-x}{2} = \frac{y+x}{2} < \frac{2y}{2} = y$. ∎

Thm. If $x, y \in \mathbb{R}$, $x<y$, then there is $s \in \mathbb{R} \setminus \mathbb{Q}$ s.t. $x < s < y$.

Pf. By above theorem, $\exists q \in \mathbb{Q}$ s.t. $\frac{x}{\sqrt{2}} < q < \frac{y}{\sqrt{2}}$. Then $s := q\sqrt{2}$ is good. ∎

Thm. (Nested Interval Principle) Let $I_1 \supseteq I_2 \supseteq I_3 \supseteq \dots$ be a nested sequence of closed intervals in $\mathbb{R}$. Then, $\bigcap_{k \ge 1} I_k \ne \emptyset$.

Proof: For $k \in \mathbb{N}_+$, let a_k denote the left end-point of I_k, and b_k - the right one. Then, the set $\{a_k \mid k \in \mathbb{N}_+\}$ is bdd above (for instance, by b_1) and the set $\{b_k \mid k \in \mathbb{N}_+\}$ is bdd below (by a_1).
Thus, $\alpha := \sup\{a_k \mid k \in \mathbb{N}_+\}$, $\beta := \inf\{b_k \mid k \in \mathbb{N}_+\}$ are well-defined.
Claim: $\alpha \le \beta$.
For a proof by contradiction, suppose $\beta < \alpha$. Then, β is not an upper bound for $\{a_k \mid k \ge 1\}$, so we can pick a_{k_1} st. $\beta < a_{k_1} \le \alpha$. Then, in turn, a_{k_1} is not a lower bound for $\{b_k \mid k \ge 1\}$, so we can pick b_{k_2} st. $b_{k_2} < a_{k_1}$. Let $k_0 := \max\{k_1, k_2\}$. Then, $b_{k_0} \le b_{k_2} < a_{k_1} \le a_{k_0}$ (by nestedness of the interval sequence), which contradicts $a_{k_0} \le b_{k_0}$. ↯
Now, by construction, $\frac{\beta+\alpha}{2}$ is greater than or equal to a_k, $\forall k \ge 1$, and less than or equal to b_k, $\forall k \ge 1$, hence $\frac{\alpha+\beta}{2} \in I_k$, $\forall k \ge 1$. ∎