1 The real numbers

1.1 Starting out

Definition 1.1. Let M be a set. A relation R on M is called a **partial ordering** on M if and only if:

- R is reflexive $\iff \forall x \in M : xRx$
- R is anti-symmetric $\iff \forall x, y \in M : xRy \land yRx \implies x = y$
- R is transitive $\iff \forall x, y \in M : xRy \land yRz \implies xRz$

If additionally $\forall x, y \in M : xRy \lor yRx$, R is called a **total ordering** on M. We say that (M, R) is linearly/totally ordered.

Definition 1.2. Let $(M, +, \cdot)$ be a **field**. Then we say that the field is **ordered** if there exists a relation on M such that (M, R) is linearly ordered, and for all $x, y, z \in M$, the following conditions hold:

- $xRy \implies (x + z)R(y + z)$
- $0_+Rx \land 0_+Ry \implies 0_+R(x \cdot y)$

where 0_+ is the additive identity element of M.

Example 1.3. Let us now consider $M = \mathbb{Q}$ as its field, $(\mathbb{Q}, \boxplus, \boxdot)$. Define $\leq$ as follows: let $[(p, q)]_\approx$ and $[(p', q')]$ be in $\mathbb{Q}$. Without loss of generality, assume $q, q' > 0$. Now define

$$[(p, q)] \leq [(p', q')] :\iff p \odot q' \leq p' \odot q :\iff \exists n \in \mathbb{N} : p' \odot q = S^n(p \odot q')$$

Claim. *$\leq$ is a total ordering.*

Proof. Proving all laws that hold for a total ordering:

- $\leq$ is reflexive $\iff \forall x \in Q : x \leq x$. Let $x = [(p, q)]_\approx$. Then $x \leq x \iff [(p, q)]_\approx \leq [(p, q)]_\approx \iff p \odot q \leq p \odot q \iff \exists n \in \mathbb{N} : p \odot q = S^n(p \odot q)$. Let $n = 0$, then $p \odot q = S^0(p \odot q) = \mathrm{id}_{\mathbb{Z}}(p \odot q) = p \odot q$ which is a tautology.
- $\leq$ is anti-symmetric $\iff \forall x, y \in \mathbb{Q} : x \leq y \land y \leq x \implies x = y$. Assume the left hand side of the implication, and let $x = \dfrac{a}{b}$, $y = \dfrac{c}{d}$:

$$\begin{aligned} x \leq y \land y \leq x &\iff \frac{a}{b} \leq \frac{c}{d} \land \frac{c}{d} \leq \frac{a}{b} \\ &\iff \exists n, m \in \mathbb{N} : c \odot b = S^n(a \odot d) \land a \odot d = S^m(c \odot b) \\ &\iff c \odot b = S^n(S^m(c \odot b)) \end{aligned}$$

  In other words, $S^n \circ S^m = \mathrm{id}_{\mathbb{Z}}$, therefore $n = m = 0$. But that implies that $c \odot b = S^0(a \odot d)$ and therefore $c \odot b = a \odot d \iff \dfrac{a}{b} = \dfrac{c}{d} \iff x = y$, so $x \leq y \land y \leq x \implies x = y$.
- $\leq$ is transitive $\iff \forall x, y \in \mathbb{Q} : x \leq y \land y \leq z \implies x \leq z$. Pick $x = \dfrac{a}{b}$, $y = \dfrac{c}{d}$, $z = \dfrac{e}{f}$. Additionally, without loss of generality, we can assume that $b, d, f > 0_{\mathbb{Z}}$[1]. Now we can make the following assumptions:
  1. $x \leq y \iff \dfrac{a}{b} \leq \dfrac{c}{d} \iff \exists n \in N : c \odot b = S^n(a \odot d) = (a \odot d) \oplus \mathrm{int}(n)$
  2. $y \leq z \iff \dfrac{c}{d} \leq \dfrac{e}{f} \iff \exists m \in N : e \odot d = S^m(c \odot f) = (c \odot f) \oplus \mathrm{int}(m)$

  From this assumptions we can deduce (respectively):
  1. $c \odot b \odot f = f \odot ((a \odot d) \oplus \mathrm{int}(n)) = (f \odot a \odot d) \oplus (f \odot \mathrm{int}(n))$

[1] This has not been made rigorous as we have not properly defined $>$ for integers, but you know what I mean.

2. $e \odot d \odot b = b \odot ((c \odot f) \oplus \text{int}(m)) = (b \odot c \odot f) \oplus (b \odot \text{int}(m))$

Substituting the first statement into the second we find:

$$e \odot d \odot b = (f \odot a \odot d) \oplus (f \odot \text{int}(n)) \oplus (b \odot \text{int}(m))$$

Now let $p = (f \odot \text{int}(n)) \oplus (b \odot \text{int}(m))$. Since $f, b > 0$, $o > 0$ (this can be proven in more detail). Therefore, $\exists o \in \mathbb{N} : \text{int}(o) = p$. In other words,

$$e \odot b \odot d = (f \odot a \odot d) \oplus p = S^o(f \odot a \odot d)$$

Therefore, $f \odot a \odot d \leq e \odot b \odot d$ and thus $f \odot a \leq e \odot b$. Finally, $\dfrac{a}{b} \leq \dfrac{b}{e}$.

- Total ordering: let $x = \dfrac{a}{b}$, $y = \dfrac{c}{d}$. We know that the following statements are tautologies:

  1. $x \leq y \iff a \odot d \leq b \odot c$
  2. $y \leq x \iff b \odot c \leq a \odot d$

  So, to prove the total ordering of $\leq$ on rationals, it suffices to prove the total ordering on integers. Let $p = [(a, b)]$ and $q = [(c, d)]$. We know that the following statements are also tautologies:

  1. $p \leq q \iff \exists n \in N : b + c = S^n(a + d)$
  2. $q \leq p \iff \exists m \in N : a + d = S^m(b + c)$

  By similar reasoning again, it suffices to prove the total ordering of $\leq$ on natural numbers. We do not yet have the formal tools to prove this, though. This should probably involve induction. We have assumed however during lectures that we have defined and proven all of the mathematical operations, relations and properties on the natural numbers.

□

Note. In that proof, I used the fact that, given $a, b, c \in \mathbb{Z}$, and $c > 0_{\mathbb{Z}}$, then $a \leq b \implies a \odot c \leq b \odot c$, which I will prove right now (we have not properly defined this in class, therefore I should do that right now).

Proof. Given $a \leq b \iff \exists n \in \mathbb{N} : b = S^n(a)$, we can see that

$$b \odot c = (a \oplus \text{int}(n)) \odot c = (a \odot c) + \text{int}(n) \odot c$$

Since $c > 0$, we know that $\text{int}(n) \odot c > 0$ and thus $\exists p \in \mathbb{N} : \text{int}(p) = \text{int}(n) \odot c$. Take such p and observe that $b \odot c = S^p(a \odot c)$. Thus $a \leq b \implies a \odot c \leq b \odot c$. □

Claim. $\leq$ *is well-defined.*

Proof. Let $x = [(a, b)]$, $y = [(c, d)]$, $x' = [(a', b')]$ and $y' = [(c', d')]$. Assume $x \approx x'$ and $x' \approx y'$. Therefore, $ab' = a'b$ and $cd' = c'd$. Now also assume that $x \leq y$, i.e. $a \odot d \leq b \odot c$. We would now like to show that $x' \leq y'$, i.e. $a' \odot d' \leq b' \odot c'$. Observe that:

$$\begin{aligned}
&\iff a \odot d \leq b \odot c \\
&\iff a \odot d \odot b' \odot c' \leq b' \odot c' \odot b \odot c \\
&\iff a' \odot d' \odot b \odot c \leq b' \odot c' \odot b \odot c \\
&\iff a' \odot d' \leq b' \odot c' \\
&\iff x' \leq y'
\end{aligned}$$

□

Claim. $(\mathbb{Q}, \boxplus, \boxdot, \leq)$ *is an ordered field.*

Proof. Since $(\mathbb{Q}, \leq)$ is linearly ordered, we only have to show a few rules. Let $x, y, z \in \mathbb{Q}$, and $x = \frac{a}{b}$, $y = \frac{c}{d}$ and $z = \frac{e}{f}$. Assume, without loss of generality, that $b, d, f > 0_{\mathbb{Z}}$. Then (leaving out $\odot$, assuming it will be understood implicitely):

- By definition, $x \leq y \iff ad \leq bc$. Also, $x + z = \frac{af + be}{bf}$ and $y + z = \frac{cf + de}{df}$. We would like to show that $x + z \leq y + z$ and thus that $df(af + be) \leq bf(cf + de)$. Cancelling and distributing gives $adf + bde \leq bcf + bde$. Then (assuming we have proven this property on the integers) $adf \leq bcf$ and thus $ad \leq bc$. The proof for this property on the integers uses similar reasoning and only differs in the fact that we assume we have proven this property on the natural numbers. So, let $n, m, o \in \mathbb{N}$. Then $n \leq m \iff \exists g \in \mathbb{N} : m = S^g(n)$ and $S^o(n) \leq S^o(m) \iff \exists h \in \mathbb{N} : S^o(m) = S^h(S^o(n))$. By the commutativity of S composed with itself, we know that $S^o(S^g(n)) = S^o(S^h(n))$. Since S is injective, we know that $g = h$ and therefore $n \leq m \iff n + o \leq m + o$.
- By definition, $0 \leq x \iff 0 \odot b \leq a \odot 1$ and equivalently $0 \leq a$. By similar reasoning, $0 \leq y \iff 0 \leq c$. Their product, $0 \leq \frac{ac}{bc} \iff 0 \leq ac$, which is true.

Therefore, $(\mathbb{Q}, \boxplus, \boxdot, \leq)$ is an ordered field. □

Definition 1.4. The **real numbers** $\mathbb{R}$ are an **ordered field** $(\mathbb{R}, +, \cdot, \leq)$ which satisfies the completeness axiom, which states that $\forall X, Y \subseteq \mathbb{R}$ such that $x, y \neq \varnothing$ and $\forall x \in X, y \in Y : x \leq y$, there exists a $c \in \mathbb{R}$ such that

$$\forall x \in X, y \in Y : x \leq c \leq y$$

Remark 1.5.
- Is $\mathbb{R}$ unique? For now, the answer to this question is unclear. Later, we will see that yes, $\mathbb{R}$ is unique to some extent (possibly by showing that for each 'implementation' of the real numbers, on its elements there exists an isomorphism between itself and any other implementation)
- This is an axiomatic way of defining $\mathbb{R}$
- Therefore, it is even unclear whether such an $\mathbb{R}$ even exists / could exist! Later we will define such an $\mathbb{R}$ in terms of so-called Dedekind cuts.
- $\mathbb{Q}$ and its field satisfies the conditions of an ordered field, but does not satisfy the completeness axiom
- There are many equivalent versions of the completeness axiom, for example, the supremum axiom.

1.2 Simple facts of $\mathbb{R}$

From now on, $0 := 0_+$ and $1 := 1_\cdot$. Also, $a \geq b :\iff b \leq a$ and $a < b :\iff a \leq b \wedge a \neq b$. Analogously, $a > b :\iff b < a$. $\leq$ and $\geq$ are called 'less/greater than or equal', and $<$ and $>$ are called 'strictly less/greater than'.

Facts 1.6.
1. 0_+ and 1_+ are unique in $\mathbb{R}$ (proof needed)
2. Let $a, b \in \mathbb{R}$. Then $a + x = b$ has a unique solution $x = b + (-a)$. Proof: by I^+, we know that $a + (-a) = 0$. Therefore, starting from the equation of the solution and adding a to both sides, we find $x + a = b + 0 = b$ and by C^+ we know that $a + x = b$.
3. $a \neq 0$, then the equation $a \cdot x = b$ has a unique solution $x = b \cdot a^{-1}$. Proof: by $I^\cdot$, we know that $a \cdot a^{-1} = 1$. Multiplying by a on both sides of the solution we find that $x \cdot a = b \cdot 1$, which by $C^\cdot$ and $N^\cdot$, $a \cdot x = b$.
4. $x \in \mathbb{R}$, $x \cdot 0 = 0 \cdot x = 0$. Proof: by N^+, $x \cdot 0 = x \cdot (0 + 0)$. Then by $D^{+,\cdot}$, $x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$. Adding $-(x \cdot 0)$ on both sides results in $x \cdot 0 + (-(x \cdot 0)) = x \cdot 0$. By I^+, $0 = x \cdot 0$. And finally by $C^\cdot$, $0 = 0 \cdot x$.
5. $x \cdot y = 0 \implies x = 0 \vee y = 0$. Proof: consider two cases:

- $y = 0$: then $x \cdot y = x \cdot 0 = 0$ and the statement is true;
- $y \neq 0$, then by the third fact, we know that $x = 0 \cdot y^{-1}$. By the fourth fact we then know that $x = 0$

6. $-x = (-1) \cdot x$. That is, the inverse element of x is the product of the inverse element of the multiplicative identity and x. We know that $x+(-x) = 0$ and that $1+(-1) = 0$. $x \cdot (1+(-1)) = x \cdot 0$, then by $D^{+,\cdot}$, $N^{\cdot}$ and the fourth fact, $x + (-1) \cdot x = 0$. By I^{+} again we know that $-x = (-1) \cdot x$.

   Similarly, $(-x) \cdot (-x) = x \cdot x$. Equivalently (by $C^{\cdot}$), $(-1) \cdot (-1) \cdot x \cdot x = x \cdot x$. Now, $(-1) \cdot (-1) = -(-1)$ by the rule we just proved. We know that $-1 + (-(-1)) = 0$ and therefore $-(-1) = 1$. Thus $(-1) \cdot (-1) \cdot x \cdot x = x \cdot x$ is a tautology, hence proven.

Facts 1.7. 1. We always have $x < y \mid x = y \mid x > y$. Proof: it suffices to show that if one of the operands of the expression is true, the others are false.

   (a) $x < y$, this means that $x \leq y \wedge x \neq y$. And one of the conditions of $x > y$ is that $y \leq x$. But $x \leq y \wedge y \leq x \implies x = y$ which is contradictory.

   (b) $x = y$. Since we have proven the above case we at least know that $\neg(x < y)$. For the case of $x > y$, this means that $x \geq y \wedge x \neq y$, which is contradictory.

   (c) $x > y$. Since we have proven the previous two cases, we already know that $\neg(x < y) \wedge \neg(x = y)$, hence proven.

2. $(x < y \wedge y \leq z) \implies (x < z)$. Proof:

$$\begin{aligned} x < y \wedge y \leq z &\iff x \leq y \wedge x \neq y \wedge y \leq z \\ &\implies x \leq y \wedge y \leq z \\ &\iff x \leq z \qquad \text{by transitivity} \end{aligned}$$

   Now suppose $x = z$. Then

$$\begin{aligned} & x < y \wedge y \leq z \\ \iff & z < y \wedge y < z \\ \iff & z \leq y \wedge z \neq y \wedge y \leq z \wedge y \neq z \\ \iff & z \leq y \wedge y \leq z \wedge y \neq z \\ \iff & y = z \wedge y \neq z \qquad \text{by antisymmetry} \end{aligned}$$

   which is always false, thus by contradiction $x \neq z$, hence proven.

3. $x < y \implies x + z < y + z$. This proof is trivial since this property already holds for $\leq$ by the properties of an ordered field. By this property, $0 < x \iff -x < 0$. In other words, this proves why the inequality sign 'flips'.

   $x \leq y \wedge z \leq w \implies x + z \leq y + w$, e.g. the property of adding inequalities. If $z = w$ this proof follows directly from the properties of an ordered field and is trivial, therefore assume $z \neq w$. We can construct, by the definition of an ordered field, the following inequalities that hold:

   - $x + z \leq y + z$
   - $y + z \leq y + w$

   By transitivity, $x + z \leq y + w$.

4. $0 < x \wedge 0 < y \implies 0 < xy$.

$$\begin{aligned} 0 < x \wedge 0 < y &\iff (0 \leq x \wedge x \neq 0) \wedge (0 \leq y \wedge y \neq 0) \\ &\implies (0 \leq xy) \wedge (xy \neq 0) \quad \text{by ordered field} \\ &\iff 0 < xy \end{aligned}$$

$x < 0 \wedge y < 0 \implies 0 < xy.$

$$\begin{aligned} x < 0 \wedge y < 0 &\iff (x \leq 0 \wedge x \neq 0) \wedge (y \leq 0 \wedge y \neq 0) \\ &\iff (0 \leq (-x) \wedge x \neq 0) \wedge (0 \leq (-y) \wedge y \neq 0) \\ &\implies (0 \leq (-x)(-y)) \wedge (xy \neq 0) \quad \text{by ordered field} \\ &\iff (0 \leq xy) \wedge (xy \neq 0) \\ &\iff 0 < xy \end{aligned}$$

$x < 0 \wedge y > 0 \implies xy < 0.$

$$\begin{aligned} x < 0 \wedge y > 0 &\iff (x \leq 0 \wedge x \neq 0) \wedge (0 \leq y \wedge y \neq 0) \\ &\iff (0 \leq (-x) \wedge x \neq 0) \wedge (0 \leq y \wedge y \neq 0) \\ &\implies (0 \leq (-x)y) \wedge (xy \neq 0) \quad \text{by ordered field} \\ &\implies (0 \leq -(xy)) \wedge (xy \neq 0) \\ &\implies (xy \leq 0) \wedge (xy \neq 0) \\ &\iff xy < 0 \end{aligned}$$

5. $0 < 1$. $0 < 1 \implies 0 \leq 1$ so let us prove the truthness of this statement by disproving $0 > 1$. By the property we have just proven, $1 < 0 \implies 0 < 1 \cdot 1 = 1$, which is a contradiction.

6. $0 < x \implies 0 < x^{-1}$. By $I^{\cdot}$, we know that $x \cdot x^{-1} = 1$. By contradiction, suppose $\neg(0 < x^{-1})$, in other words, since the multiplicative inverse is not zero, $0 > x^{-1}$. By one of our rules, these assumptions imply that $x \cdot x^{-1} < 0$, e.g. $1 < 0$, which is a contradiction.

   $(0 < x \wedge x < y) \implies (0 < y^{-1} \wedge y^{-1} < x^{-1})$. By the assumption, we know $x \neq y$ and $x \neq 0$. Then by transitivity we know that $0 \leq y$. If $y = 0$ then $0 < x \wedge 0 > x$ which is false, so $y \neq 0$ and thus $0 < y$. Therefore we already know $0 < y^{-1}$ and $0 < x^{-1}$. Starting at $x < y$ and multiplying both sides by both inverses, we find that $x \cdot x^{-1} \cdot y^{-1} < y \cdot x^{-1} \cdot y^{-1}$ or in other words $y^{-1} < x^{-1}$ (by $C^{\cdot}$ and $I^{\cdot}$).

1.3 Completeness axiom and its consequences

Definition 1.8. A subset X of $\mathbb{R}$ is called **bounded above** if there exists a $c \in \mathbb{R}$ such that $\forall x \in X : x \leq c$. Any such c is an **upper bound** of X.
A subset X of $\mathbb{R}$ is called **bounded below** if there exists a $c \in \mathbb{R}$ such that $\forall x \in X : x \geq c$. Any such c is a **lower bound** of X.
An upper/lower bound of X is called **maximal/minimal** if it is an element of X. Such elements may not exist for any bound. These elements are denoted $\max X$ and $\min X$, respectively.

Definition 1.9. The smallest upper/lower bound of $X \subseteq \mathbb{R}$ is called the **supremum/infemum** of X denoted by $\sup X$ and $\inf X$, respectively.
(editor's note) Suppose $\inf X = u$. This means that, if c is another upper bound of X, then $c \geq u$.

Note.

$$\sup M = \min\{c \in \mathbb{R} \mid \forall x \in M : x \leq c\}$$
$$\inf M = \max\{c \in \mathbb{R} \mid \forall x \in M : x \geq c\}$$

if the max or min exists, of course.

Note. A set $X \subseteq \mathbb{R}$ is called **bounded** if it has an upper and a lower bound.

Theorem 1.10. *Any bounded above, nonempty $A \subseteq \mathbb{R}$ has a supremum.*

Proof. Let $Y := \{y \in \mathbb{R} \mid \forall x \in X : x \leq y\}$. Suppose $a \in \mathbb{R}$ is an upper bound of A, in other words, $\forall x \in X : x \leq a$. Therefore, $a \in Y$, and Y is thus nonempty. For that reason, by the completeness axiom, we can find a $c \in \mathbb{R}$ such that $\forall x \in X, y \in Y : x \leq c \leq y$. By this criterion, $c \in Y$, and c is also an upper bound of X. I claim that for such a c, $\sup X = c$. In other words, if d is another upper bound of X, $(\forall x \in X : x \leq d) \wedge d \geq c$. By the definition of Y, equivalently, $d \in Y \wedge c \leq d$, which is a true proposition by the completeness axiom. $\square$

Note: while still in the same section, lecture two notes start here

Claim. *Minimal/maximal elements, if they exist, are unique.*

Proof. Let x, y be minimums of a set M, that is, $\min M = x \wedge \min M = y$. In other words, $\forall z \in M : z \leq z \wedge y \leq z \wedge x, y \in M$. Since x, y are also elements of M, we can substitute $z = x$ and $z = y$. Therefore, $y \leq x \wedge x \leq y$. By antisymmetry of $\leq$, we then know that $x = y$. Therefore, given two minimums of a set, they are always equal to each other, and therefore unique. □

Reformulation of supremum axiom/theorem. *Any bounded above, nonempty $X \subseteq \mathbb{R}$ has a unique supremum.*

Proof. (as presented in the lecture instead). Because of the uniqueness of min, it suffices to show that there is a minimal element of $Y := \{y \in \mathbb{R} \mid \forall x \in X : x \leq y\}$. Since X is bounded, we know that Y has at least one element by its definition. We also know that $\forall x \in X, y \in Y : x \leq y$, so we are allowed to invoke the completeness axiom and find a c such that $\forall x \in X, y \in Y : x \leq c \leq y$. Therefore, c is an upper bound of X. Suppose we know that there exists some other upper bound of X, c'. This means that $c' \in Y$ and therefore $c \leq c'$, so $\sup X = c$. □

Remark 1.11. This theorem is equivalent to the completeness axiom, it is provable that this theorem implies the completeness axiom. For that reason the axiom is sometimes formulated as this theorem instead, and is called the 'supremum axiom'.

Example 1.12. Let $M := \{x \in \mathbb{R} \mid 0 \leq x < 1\}$. Obviously, 0 is a lower bound and 1 is an upper bound. We know that $0 \in M$, so $\min M = 0$, and therefore also $\inf M = 0$. Now let us consider the supremum. Clearly, $\sup M \leq 1$ since 1 is an upper bound. Claim: $\sup M = 1$. This means that, if $x \in M$[2] is an upper bound, we can find a $q \in M$ such that $x < q < 1$. Intuitively, a good candidate is the arithmetic mean, so let $q = 2^{-1} \cdot (x+1)$ [3]. Observe that $x < q \iff x < 2^{-1} \cdot (x+1) \iff 2x < x+1 \iff x < 1$ which is a tautology since $x \in M$. Similarly, $q < 1 \iff 2^{-1} \cdot (x+1) < 1 \iff x + 1 < 2 \iff x < 1$ which is again a tautology. Thus $\sup M \geq 1 \wedge \sup M \leq 1$ and by antisymmetry, $\sup M = 1$.

Example 1.13. We will discuss the existence of square roots. **Claim.**

$$\forall y \in \mathbb{R} : (y \geq 0 \implies \exists! x \in \mathbb{R} : x \cdot x = y \wedge x \geq 0)$$

Strategy. Construct a set in $\mathbb{R}$ such that its supremum is equal to $\sqrt{y} = x$. Consider

$$M := \{z \in \mathbb{R} \mid 0 \leq z \cdot z \leq y\}$$

Subclaim. $x := \sup M$ satisfies $x \cdot x = y$.
Proof. x exists be the boundedness of M, and $0 \in M$, so M is nonempty. Without loss of generality, assume $0 \leq y < 1$. Then, $0 \leq z < 1$, and $0 \leq z \wedge 0 \leq z \implies 0 \leq z \cdot z$, therefore $0 \leq z^2 \leq z < 1$. By one of the proven facts, we know that $x^2 < y \mid x^2 = y \mid x^2 > y$. If $x^2 = y$ we have already proven the claim. We shall now find contradictions for the other cases to rule them out and prove the claim for all cases:

- **Case 1**: $x^2 < y$. Let $\varepsilon := \min\{(y - x^2)(2x + 1)^{-1}, 1\}$. So, $0 < \varepsilon \leq 1$. Let $z := x + \varepsilon$. Since $\varepsilon > 0$, $z > x$. Observe that

$$\begin{aligned} z^2 &= x^2 + 2\varepsilon x + \varepsilon^2 \\ &= x^2 + (2x + \varepsilon)\varepsilon \\ &\leq x^2 + (2x + 1)\varepsilon \\ &\leq x^2 + y - x^2 \\ &= y \end{aligned}$$

  e.g. $z^2 \leq y$, thus $z \in M$, yet $z > x$ but by definition $x = \sup M$, which is a contradiction.

[2] Which can be asserted since we have already shown 1 to be an upper bound, so a smaller one better be in M
[3] Here, 2 is just a shorthand for denoting $1 + 1$

- **Case 2**: $x^2 > y$. Let $\varepsilon := (2x)^{-1} \cdot (x^2 - y)$. So, $0 < \varepsilon$. Let $z := x - \varepsilon$. Since $\varepsilon > 0$, $z < x$. Observe that

$$\begin{aligned} z^2 &= x^2 - 2x\varepsilon + \varepsilon^2 \\ &> x^2 - 2x\varepsilon \\ &= x^2 - x^2 + y \\ &= y \end{aligned}$$

  e.g. $z^2 > y$. This means that $z \notin M$, but $0 \leq z^2 < x = \sup M$, which is a contradiction.

Now let us prove the uniqueness of the square root: let $x, x' \in \mathbb{R}$ and $x, x' > 0$. Assume $x^2 = y = x'^2$. Since $x^2 - x'^2 = 0$, $0 = x^2 - x'^2 = x^2 + xx' - xx' + x'^2 = (x + x')(x - x')$. Since $x + x' \geq 0$, $x - x' = 0$ and thus $x = x'$. Finally, consider the case where either x or x' (so, without loss of generality, assume $x = 0$), then $x^2 = 0$ and $x'^2 = 0$ and so $x' = 0$ and $x = x'$.

Theorem 1.14. $\forall n \in \mathbb{N}^* : \forall y \in \mathbb{R} : \exists! x \geq 0 : x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}} = y$

1.4 $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ in $\mathbb{R}$

Recall: In the foundations of mathematics, we constructed $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ according to:

- $\mathbb{N}$ by the axiom of infinity
- $\mathbb{Z}$ as the quotient set of $(\mathbb{N} \times \mathbb{N})$ under $\sim$
- $\mathbb{Z}$ as the quotient set of $(\mathbb{Z} \times \mathbb{Z})$ under $\approx$

Convention: $f(A)$ where $f : X \to Y$ is a map and $A \subseteq X$ is a set $\{y \in Y \mid \exists x \in A : f(x) = y\}$. In other words, $f(A)$ is the image of applying f to all elements of A. Define $\text{rat} : \mathbb{Z} \to \mathbb{Q}$ such that $[(a, b)]_\sim \mapsto [(a - b, 1)]_\approx$. Now, $\text{rat}(\text{int}(\mathbb{N})) \subseteq \mathbb{Q}$. With invisible ink: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$.

Definition 1.15.

$$\begin{gathered} S : \mathbb{R} \to \mathbb{R} \\ x \mapsto x + 1_{\mathbb{R}} \\ f : \mathbb{Z} \to \mathbb{R} \\ [(m, n)] \mapsto \begin{cases} S^{m-n}(0_{\mathbb{R}}) & \text{if } m > n, \\ S^{n-m}(0_{\mathbb{R}}) & \text{if } m < n, \\ 0_R & \text{otherwise.} \end{cases} \\ g : \mathbb{Q} \to \mathbb{R} \\ [(p, q)] \mapsto f(p) \cdot f(q)^{-1} \end{gathered}$$

Furthermore, we throw out the beautiful notation that Frederic introduced and from now on exclude 0 from $\mathbb{N}$, calling $g(\mathbb{N}^*)$ the natural numbers in $\mathbb{R}$. As in the lecture notes:

- $g(\mathbb{N}^*)$ is called the natural numbers in $\mathbb{R}$ and we use the notation $\mathbb{N}^*$,
- $g(\mathbb{Z})$ is called the integers in $\mathbb{R}$ and we use the notation $\mathbb{Z}$.
- $g(\mathbb{Q})$ is called the rational numbers in $\mathbb{R}$ and we use the notation $\mathbb{Q}$.

Lemma 1.16. *f, g are well-defined and are embeddings of $\mathbb{Z}$ and $\mathbb{Q}$ in $\mathbb{R}$ (e.g. monomorphisms).*

Proof. The proof of the properties of an embedding is tedious, so we will only show the injectivity of g. Let $[(a, b)]$ and $[(a', b')]$ be in $\mathbb{Z}$. Assume that $f([(a, b)]) = f([(a', b')])$. This means that $f(a) \cdot f(b)^{-1} = f(a') \cdot f(b')^{-1}$. In other words, $f(a) \cdot f(b') = f(a') \cdot f(b)$. One property (that we leave unproven) of f is that $f(a) \cdot f(b) = f(ab)$, so $ab' = a'b$ or in other words, $(a, b) \sim (a', b')$ which means that $[(a, b)] = [(a', b')]$. $\square$

Definition 1.17. Let A be a set. If $A \subseteq \mathbb{R}$ and $\forall x \in A : x + 1_{\mathbb{R}} \in A$, A is called **inductive**.

Lemma 1.18. $g(\mathbb{N}) := g(\text{rat}(\text{int}(\mathbb{N})))$ *is the smallest*[4] *inductive set containing* $0_{\mathbb{R}}$.

Proof. $g(\mathbb{N})$ is inductive: let $n \in \mathbb{N}$, then $S(n) \in \mathbb{N}$ by the axiom of infinity. Clearly, $g(n), g(S(n)) \in g(\mathbb{N})$. $g(n) = f(n) \cdot 1^{-1} = f(n) = S^n(0_{\mathbb{R}})$ and $g(S(n)) = \ldots = S^{n+1}(0_{\mathbb{R}}) = S^n(0_{\mathbb{R}}) + 1_{\mathbb{R}}$ which by definition proves that $g(\mathbb{N})$ is inductive.
$0_{\mathbb{R}} \in g(\mathbb{N})$: $g(\varnothing) = f(0_{\mathbb{Z}}) = id_{\mathbb{R}}(0_{\mathbb{R}}) = 0_{\mathbb{R}}$.
Consider another set $M \subseteq \mathbb{R}$ such that M is inductive and contains $0_{\mathbb{R}}$. We would like to show that for any such set, $g(\mathbb{N}) \subseteq M$. Let $S := \{n \in \mathbb{N} \mid g(n) \in M\}$, so $S \subseteq M$. It rests to show that $S = \mathbb{N}$. Clearly, $\varnothing \in S$ because $g(\varnothing) = 0_{\mathbb{R}} \in M$. Now, for all $n \in S$, we have that $S(n) \in S$ since $g(S(n)) \in M$ by the property of induction. Thus S satisfies the axiom of infinity and $S = \mathbb{N}$, which directly implies that $g(\mathbb{N}) \subseteq M$. □

Remark 1.19.
- Since g is injective, 'leaving out the invisible chalk' is justified since '$g(\mathbb{N}) = \mathbb{N}$' is not ambiguous.
- In Analysis I the natural numbers (sadly) exclude $0_{\mathbb{R}}$. If we would refer to $\mathbb{N}$ as defined in the foundations of mathematics, we write $\mathbb{N}_0$.

Corollary 1.20. *Principle of mathematical induction: Any inductive* $A \subseteq \mathbb{N}^*$ *such that* $1_{\mathbb{R}} \in A$ *equals* $\mathbb{N}^*$.

Example 1.21. Define $s_n := s_{n-1} + n$, $s_1 := 1$. In other words, $s_n = \sum_{i=1}^{n} i$. Now let $s'(n) := n(n+1)2^{-1}$. We would like to show that $s = s'$. Consider the set $M := \{n \in N^* \mid s_n = s'(n)\}$. It now suffices to show that $M = \mathbb{N}^*$, which we can do by proving the properties of $\mathbb{N}$. Clearly, $M \subseteq N^*$. Furthermore, $1 \in M \iff s_1 = s'(1) \iff 1 = 1(1+1)2^{-1} = 1$, so $1 \in M$. Lastly, suppose $x \in M$, so $s_x = s'(x)$. Consider:

$$\begin{aligned} s_{x+1} &= s_x + x + 1 \\ &= s'(x) + x + 1 \\ &= x(x+1)2^{-1} + (x+1) \\ &= (x \cdot 2^{-1} + 1)(x+1) \\ &= (x+1)(x+2)2^{-1} \\ &= s'(x+1) \end{aligned}$$

Therefore $s_x = s'(x) \implies s_{x+1} = s'(x+1)$, which proves that M is inductive and contains $1_{\mathbb{R}}$. For that reason, $M = \mathbb{N}^*$.

Definition 1.22. Every $x \in \mathbb{R}$ such that $x \notin g(\mathbb{Q})$ is called **irrational**. Furthermore, the set of irrational numbers is thus $\mathbb{R} \setminus \mathbb{Q}$.

Theorem 1.23. *The set of irrational numbers is nonempty.*

Proof. We would like to show that $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$. By an earlier theorem, we know that $\sqrt{2}$ is unique and is an element of $\mathbb{R}$. It thus suffices to show that $\sqrt{2} \notin \mathbb{Q}$. By way of contradiction, suppose that $\sqrt{2} \in \mathbb{Q}$. For that reason, we know that we can write $\sqrt{2} = [(p,q)]_{\approx}$. Without loss of generality, assume $p, q \geq 0$. So, using some invisible chalk, we can write $2 = \frac{p^2}{q^2} \iff p^2 = 2q^2$.

- If $p = 2k$ and $q = 2l$ for some k, l (in other words, p and q are even), we know that $[(k,l)] = [(p,q)]$. So without loss of generality we can assume not both p and q are even.
- If $p = 2k+1$ and $q = 2l+1$, we can see that $2k+1 = 2(4l^2+4l+1)$ and thus $2k = 8l^2+8l+1$, and such a k is not in $\mathbb{Z}$, so without loss of generality we can assume not both p and q are odd.
- **Case 1**: p is even, in which case $p = 2k$ and $q = 2l+1$. So, $2k^2 = 4l^2+4l+1$. Such a k again does not exist in $\mathbb{Z}$, which is a contradiction.

[4] This means that for any other set A satisfying the condition, $g(\mathbb{N}) \subseteq A$

- **Case 2**: q is even, in which case $q = 2k$ and $p = 2l + 1$. So, $4l^2 + 4l + 1 = 8k^2$, and again such a k does not exist in $\mathbb{Z}$, which is a contradiction.

Therefore, for any choice of p and q, $[(p, q)] = \sqrt{2}$ generates a contradiction, so $\sqrt{2} \notin \mathbb{Q}$. Thus the set of irrationals is nonempty. □

Facts 1.24.
- $\forall n, m \in \mathbb{N}^* : n + m \in \mathbb{N}^*$, since $g(n) + g(m) = g(n + m)$.
- $\forall n \in \mathbb{N}^* : n \neq 1 \implies n - 1 \in \mathbb{N}^*$
- $\forall n \in \mathbb{N}^* : \min\{x \in N^* : n < x\} = n + 1$
- $\forall n, m \in \mathbb{N}^* : n < m \implies n + 1 \leq m$
- $\forall n \in N^* : \nexists x \in N^* : n < x < n + 1$
- $\forall n \in \mathbb{N}^* : n - 1$ is the predecessor of n.
- $\forall A \subseteq \mathbb{N} : \min(A)$ exists.

1.5 Archimedean principle

Facts 1.25.
- Every bounded above $A \subseteq \mathbb{N}^*$ has a maximum element. Proof: got messed up by the lecturer lol.
- $\mathbb{N}^*$ is **not** bounded above. Proof: suppose $c \in \mathbb{R}$ is an upper bound of $\mathbb{N}^*$. Thus, $\forall n \in \mathbb{N}^* : n \leq c$. Consider the set $S := \{n \in \mathbb{N}^* \mid n \leq c\}$. S is a subset of $\mathbb{N}^*$, so consider $n := \max S$. We know that $n \leq c$. Trivially, $n + 1 > n$ so $n + 1 > c$. But $n + 1 \in \mathbb{N}^*$, so c is not an upper bound.
- Similarly, $\mathbb{Z}$ is not bounded below or above.
- Any nonempty bounded below subset of $\mathbb{Z}$ has a minimal element.

Theorem 1.26. $\forall x \in \mathbb{R} : \forall \overbrace{h}^{\in \mathbb{R}} > 0 : \exists! k \in Z : (k - 1)h \leq x < kh$.

Proof. Consider the set $M := \{n \in \mathbb{Z} \mid x < nh\}$. Then M is nonempty and bounded below by $\frac{x}{h}$. So we can find some $k := \min M$. Therefore, $k \in M$ but $k - 1 \notin M$. k already satisfies the right hand side of the inequality, so we only have to prove the left hand side. Consider the fact that $k - 1 \notin M$ implies $\neg(x < (k - 1)h)$ so $(k - 1)h \leq x$. □

Facts 1.27.
- $\forall \varepsilon > 0 : \exists n \in \mathbb{N}^* : 0 < \frac{1}{n} < \varepsilon$. Proof: By the Archimedean principle, we can find a unique $n \in \mathbb{Z}$ such that $1 < k\varepsilon$. Since $\varepsilon > 0$, $k > 0$ and $k \in \mathbb{N}^*$. Thus $0 < \frac{1}{k} < \varepsilon$.
- $\forall x \in \mathbb{R} : x \geq 0 \wedge \forall n \in \mathbb{N}^* : x < \frac{1}{n} \implies x = 0$. Proof: suppose $x > 0$ (bwoc). Then we can find $n \in \mathbb{N}^*$ such that $0 < \frac{1}{n} < x$, which contradicts the assumption.
- $\forall a, b \in \mathbb{R} : (a < b) \implies \exists r \in \mathbb{Q} : a < r < b$ (density of the rational numbers in $\mathbb{R}$). PRoof: find $n \in \mathbb{N}^*$ such that $\frac{1}{n} < b - a$, since $a < b \iff 0 < b - a$. Then according to the Archimedean principle, find $k \in \mathbb{Z}$ such that $a < \frac{k}{n}$. It now suffices to show $\frac{k}{n} < b$. (I have done this on the problem sheet)
- $\forall x \in \mathbb{R} : \exists! z \in \mathbb{Z} : z \leq x < z + 1$. Note: Such a z is called 'the integer part of x' or equivalently, $\lfloor x \rfloor = z$. Proof: first, let us construct such a z. Well, since $1 > 0$, find $z \in \mathbb{Z}$ such that $z - 1 \leq x < z$. Then, $z \leq x < z + 1$.

1.6 Completeness axiom and its consequences (2)

Definition 1.28. Let X be a set. A map $A : \mathbb{N}^* -> \mathcal{P}(X)$ is called a **sequence of (sub)sets** on X. We use the shorthand notation $A_1, A_2, \ldots$. Such a sequence is called **nested** iff A is 'decreasing' wrt the natural inclusion order of $\mathcal{P}(X)$. That is, $A_1 \supseteq A_2 \supseteq \ldots$.

Theorem 1.29. *(the principle of nested intervals). Let $I : \mathbb{N}^* \to \mathcal{P}(\mathbb{R})$ be a nested sequence on closed intervals in $\mathbb{R}$. That is, $I_k = [a_k, b_k] := \{x \in \mathbb{R} \mid a_k \leq x \leq b_k\}$, and $I_n \supseteq I_{n+1}$ for all $n \in \mathbb{N}^*$. Then there exists some $c \in \mathbb{R}$ such that $c \in \bigcap \operatorname{im} I$. If additionally $\forall \varepsilon > 0 : \exists k \in \mathbb{N}^* : |I_k| < \varepsilon$, where $|I_K| = |[a_k, b_k]| := b_k - a_k$, then such a c is unique.*

Proof. Assume the intervals are nonempty, e.g. $a_k \leq b_k$. Then construct the sets

$$A := \{a_k \in \mathbb{R} \mid k \in \mathbb{N}^*\}$$
$$B := \{b_k \in \mathbb{R} \mid k \in \mathbb{N}^*\}$$

By construction, $A \leq B$ (in the sense that $a_k \leq b_k$). By the completeness axiom, we can find a $c \in \mathbb{R}$ such that $\forall a \in A, b \in B : a \leq c \leq b$. So by definition of the elements of $\operatorname{im} I$, $c \in I_k$ for all $k \in \mathbb{N}^*$, thus $c \in \bigcap \operatorname{im} I$.
Next, under the additional assumption, wts that if $c, c' \in \bigcap \operatorname{im} I$, then $c = c'$. Let $\varepsilon = |c - c'|$, find $k \in \mathbb{N}^*$ such that $b_k - a_k < \varepsilon = |c - c'|$. Bwoc assume $c \neq c'$, wlog assume $c > c'$. Then $b_k - a_k < c - c'$. Additionally, $a_k \leq c' \wedge c \leq b_k \implies a_k + c \leq c' + b_k$ e.g. $b_k - a_k \geq c - c'$, which is a contradiction. □

1.7 Countable vs. uncountable

Definition 1.30. Let X be a set. If there exists a bijection $f : \mathbb{N}^* \to X$, then X is called **countable**. If the codomain of such a bijection is instead a bounded above subset of $\mathbb{N}^*$, then X is called **finite**.

Proposition 1.31.
- *Any infinite subset of a countable set is countable.*
- *$\bigcup A$ such that A is at most countable[5] is at most countable.*

Theorem 1.32. *$\mathbb{R}$ is uncountable.*

Proof. Suppose $\mathbb{R}$ is countable and find a suitable bijection $f : \mathbb{N}^* \to \mathbb{R}$. Now construct a $x \in \mathbb{R}$ that is not in $\operatorname{im} f$ as follows: (well, at this point the lecturer performs some vague argument that does not quite convince me at all, something with finding nested intervals in $[0, 1]$). □

2 Sequences

Definition 2.1. Let X be a set. A map $x : \mathbb{N}^* \to X$ is called a **sequence** in X. We also use the notation $(x_n)_{n \in \mathbb{N}^*}$, or in Zorich, $\{x_n\}$, or shorthand, (x_n). The set of all sequences in X is denoted by $X^{\mathbb{N}^*}$ and defined by

$$X^{\mathbb{N}^*} := \{(x : \mathbb{N}^* \to X) \in \mathcal{P}(\mathbb{N}^* \times X) \mid x \text{ is a map}\}$$

In the case where $X := \mathbb{R}$, we also say that x is a sequence of real numbers.

Definition 2.2. Let X be a set. Then a map $d : X \times X \to [0, \infty)$ is called a **distance function** or **metric** if

- $d(x, y) = 0 \iff x = y$,
- $d(x, y) = d(y, x)$,
- $d(x, z) \leq d(x, y) + d(y, z)$,

where $x, y, z \in X$. The pair (X, d) under these conditions constitutes a **metric space**.

Example 2.3. $(\mathbb{R}, (x, y) \mapsto |x - y|)$ is a metric space.

[5] finite or countable

Proof.
- $d(x,y) = 0 \iff |x-y| = 0 \iff x - y = 0 \iff x = y$.
- $d(x,y) = |x-y| = |y-x| = d(y,x)$.
- $d(x,y) + d(y,z) = |x-y| + |y-z| \geq |x-z| = d(x,z)$.

□

Example 2.4. Define the **discrete metric** d_0 on a set $X \neq \varnothing$ as follows:

$$d_0(x,y) := \begin{cases} 1 & \text{if } x \neq y \\ 0 & \text{otherwise} \end{cases}$$

Then (X, d_0) constitutes a metric space.

Proof.
- $d(x,y) = 0 \iff x = y$ by definition.
- Suppose $x = y$, then $d(x,y) = 0 = d(y,x)$. In the other case, suppose $x \neq y$. Then $d(x,y) = 1 = d(y,x)$.
- This requires lots of cases...

□

Ex NaN. Consider the sets X, Y such that $Y \subseteq X$. Then if (X,d) is a metric space, (Y,d) is a metric space.

Ex NaN. Define the metric

$$d : \mathbb{R}^d \to [0, \infty)$$

$$d((x_1, \ldots, x_d), (y_1, \ldots, y_d)) := \sqrt{\sum_{i=0}^{d} \left| x_i - y_i \right|^2}$$

Then $(\mathbb{R}^d, d)$ constitutes a metric space, where $d \in \mathbb{N}^*$ is sometimes called the **dimension** of the metric space. Yeah, totally not confusing that our distance metric has the same name as our dimension constant.

Definition 2.5. Let (X,d) be a metric space. Then a sequence $(x_n)_{n \in \mathbb{N}^*}$ is called:

- **convergent** if $\exists x \in X : \forall \varepsilon > 0 : \exists N \in \mathbb{N}^* : \forall n \in \mathbb{N}^* : (n \geq N \implies d(x_n, x) < \varepsilon)$. We say that x_n **converges to** x. Similarly, $\lim\limits_{n \to \infty} x_n = x$. The most common notation we will use is $x_n \overset{n \to \infty}{\longrightarrow} x$.
- **Cauchy** if $\forall \varepsilon > 0 : \exists N \in \mathbb{N}^* : \forall n, m \in \mathbb{N}^* : (n, m \geq N \implies d(x_n, x_m) < \varepsilon)$.
- **bounded** if $\exists c \in X : \exists M > 0 : d(c, x_n) < M$.

Remark 2.6. Work through the example of $\left(\frac{1}{n}\right)$ as a sequence in the reals. Prove that it converges to 0. Furthermore prove that $((-1)^n)$ is not convergent by formally negating the statement that it is convergent.

Proof. Let $\varepsilon > 0$, define $N := \min\{n \in \mathbb{N}^* \mid n > \frac{1}{\varepsilon}\}$, so we know that $N > \frac{1}{\varepsilon}$. Consider that if $n \geq N$, we have that $n > \frac{1}{\varepsilon}$, so $\frac{1}{n} < \varepsilon$, thus $|x_n - 0| < \varepsilon$ which proves the convergence.
TODO proof of nonconvergence of alternating sequence. □

Proposition 2.7. *Let (x_n) be a sequence in (X,d). Then (x_n) converges $\implies$ (x_n) Cauchy $\implies$ (x_n) bounded. Furthermore, limits are unique. That is,*

$$x_n \overset{n \to \infty}{\longrightarrow} x \wedge x_n \overset{n \to \infty}{\longrightarrow} y \implies x = y$$

Lastly, $x_n \overset{n \to \infty}{\longrightarrow} x$ in (X,d) $\iff$ $((d_n, x))_{n \in \mathbb{N}^*} \overset{n \to \infty}{\longrightarrow} 0$ in $(\mathbb{R}, d_2)$.

Proof. First, suppose $x_n \overset{n \to \infty}{\longrightarrow} x$. Thus we know that $\forall \varepsilon > 0 : \exists N \in \mathbb{N}^* : \forall n \geq N : d(x_n, x) < \varepsilon$. Consider that $d(x_n, x_m) \leq d(x_n, x) + d(x, x_m) = d(x_n, x) + d(x_m, x)$. In order to prove Cauchy, assume $n, m \geq N$. Thus $d(x_n, x) < \varepsilon$ and $d(d_m, x) < \varepsilon$, so $d(x_n, x_m) \leq 2\varepsilon$, hence Cauchy is proven.
Now simply assume we have a Cauchy sequence (x_n). Take any $\varepsilon > 0$, and find its corresponding N. Consider that $\varepsilon > d(x_n, x_N) \geq d(x_n, M)+$. □

A Note

The proofs have not been verified by anyone but myself.