UMA204: Introduction to Basic Analysis

Naman Mishra

January 2024

Contents

Lecture 01: Mon 01 Jan '24

0 The course

Instructor: Prof. Purvi Gupta
Office: L-25
Office hours: Wed 17:00–18:00
Lecture hours: MW 12:00–12:50, Thu 9:00–9:50
Tutorial hours: Fri 12:00–12:50

We assume the following.

- Basics of set theory
- Existence of $\mathbb{N} = \{0, 1, 2, \ldots\}$ with the usual operations $+$ and $\cdot$

For a recap, refer lectures 1 to 3 of UMA101.

1 Number Systems

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

1.1 The Naturals

(Recall from UM101) $\mathbb{N}$ is the unique minimal inductive set granted by the ZFC axioms. Addition and multiplication are defined by the recursion principle and we showed that they

- are associative and commutative,
- admit identity elements 0 and 1 respectively,
- satisfy the distributive law,
- satisfy cancellation laws,
- but do not admit inverses.

1.2 Relations

(Recall) A relation on a set A is a subset $R \subseteq A \times A$. We write $a \mathrel{R} b$ to denote $(a, b) \in R$.

Definition 1.1 (Partial order)**.** A relation R on A is called a *partial order* if it is

- reflexive – $a \mathrel{R} a$ for all $a \in A$;
- antisymmetric – if $a \mathrel{R} b$ and $b \mathrel{R} a$ then $a = b$ for all $a, b \in A$;
- transitive – if $a \mathrel{R} b$ and $b \mathrel{R} c$ then $a \mathrel{R} c$ for all $a, b, c \in A$.

Additionally, if for all $x, y \in A$, $x \mathrel{R} y$ or $y \mathrel{R} x$, then R is called a *total order*.

A set A equipped with a partial order $\leq$ is called a *partially ordered set* (or *poset*).
A set A equipped with a total order $\leq$ is called a *totally ordered set* or simply an *ordered set*.

Examples.

- $(\mathbb{N}, \leq)$ where we say that $a \leq b$ if $\exists\, c \in \mathbb{N}$ such that $a + c = b$.
- $(\mathbb{N}, |)$ where we say that $a \mid b$ if $\exists\, c \in \mathbb{N}$ such that $a \cdot c = b$.

In UMA101, we defined order slightly differently, where we said that either $a < b$ or $b < a$ but never both. This is a "strict order". We will denote a weak partial order by $\leq$ and a strict partial order by $<$. (the notation is suggestive of how to every order there is a corresponding strict order and vice versa).

Definition 1.2 (Equivalence)**.** An *equivalence relation* on a set A is a relation R satisfying

- reflexivity;
- symmetry – if $a \ R \ b$ then $b \ R \ a$ for all $a, b \in A$;
- transitivity.

Notation. We write $[x]_R$ to denote the set $\{y \in A \mid x \ R \ y\}$.

Proposition 1.3. The collection $\mathscr{A} = \{[x]_R \mid x \in A\}$ partitions A under any equivalence relation R on A.

Proof. For every $x \in A$, $x \in [x]_R$ and so $\bigcup \mathscr{A} = A$.

Let $[x]_R \cap [y]_R \neq \varnothing$, where $x, y \in A$. Then there exists $z \in A$ such that $x \ R \ z$ and $y \ R \ z$, from which it follows that $x \ R \ y$ and $[x]_R = [y]_R$. □

1.3 The Integers

We cannot solve $3 + x = 2$ in $\mathbb{N}$. We introduce $\mathbb{Z}$ to solve this problem.

Consider the relation R on $\mathbb{N} \times \mathbb{N}$ given by

$$(a, b) \ R \ (c, d) \iff a + d = b + c.$$

(check that this is an equivalence relation trivial).

Definition 1.4. We define $\mathbb{Z}$ to be the set of equivalence classes of R, notated $\mathbb{N} \times \mathbb{N}/R$.

Further, define

- $[(a, b)] +_{\mathbb{Z}} [(c, d)] \coloneqq [(a + c, b + d)]$;
- $[(a, b)] \cdot_{\mathbb{Z}} [(c, d)] \coloneqq [(ac + bd, ad + bc)]$.
- $z_1 \leq_{\mathbb{Z}} z_2$ iff there exists $n \in \mathbb{N}$ such that $z_1 +_{\mathbb{Z}} [(n, 0)] = z_2$ (alternatively, $[(a, b)] \leq_{\mathbb{Z}} [(c, d)]$ iff $a + d \leq b + c$).

We need to check that these are well-defined. What does this mean? Consider

$$[(1, 2)] +_{\mathbb{Z}} [(3, 4)] = [(4, 6)]$$
$$[(3, 4)] +_{\mathbb{Z}} [(3, 4)] = [(6, 8)]$$

Our definition must ensure that $[(4,6)] = [(6,8)]$.
In general, the definitions are well-defined if they are independent of the choice of representatives. Throughout this section, we will omit the parentheses in $[(a,b)]$ and write it as $[a,b]$.

Lecture 02: Tue 02 Jan '24

> **Proposition 1.5.** The operations $+_{\mathbb{Z}}$, $\cdot_{\mathbb{Z}}$ and the relation $\leq_{\mathbb{Z}}$ are well-defined.

Proof. Suppose $x = [a,b] = [a',b']$ and $y = [c,d] = [c',d']$. Then

$$\begin{aligned} a + b' &= a' + b \\ c + d' &= c' + d \\ (a+c) + (b'+d') &= (a'+c') + (b+d) \\ (a+c, b+d) &\ R\ (a'+c', b'+d') \\ [a+c, b+d] &= [a'+c', b'+d'] \end{aligned}$$

Since $\leq_{\mathbb{Z}}$ is defined in terms of $+_{\mathbb{Z}}$, it is also well-defined. For multiplication,

$$\begin{aligned} (a+b')c + (a'+b)d &= (a'+b)c + (a+b')d \\ (ac+bd) + (a'd+b'c) &= (a'c+b'd) + (ad+bc) \\ [ac+bd, ad+bc] &= [a'c+b'd, a'd+b'c] \end{aligned}$$

and symmetrically

$$[a'c+b'd, a'd+b'c] = [a'c'+b'd', a'c'+b'd']$$

so by transitivity

$$[ac+bd, ad+bc] = [a'c'+b'd', a'c'+b'd'] \qquad \square$$

> **Proposition 1.6.** The relation $\leq_{\mathbb{Z}}$ is a total order on $\mathbb{Z}$.

Proof. Let $x = [a,b], y = [c,d] \in \mathbb{Z}$. Since $x +_{\mathbb{Z}} [0,0] = [a+0, b+0] = x$, $x \leq_{\mathbb{Z}} x$.

Suppose $x \leq_{\mathbb{Z}} y$ and $y \leq_{\mathbb{Z}} x$. Then there exist $m, n \in \mathbb{N}$ such that $x + [m,0] = y$ and $y +_{\mathbb{Z}} [n,0] = x$. Thus $x +_{\mathbb{Z}} [m,0] +_{\mathbb{Z}} [n,0] = [a+m+n, b] = [a,b]$. This gives $a+m+n+b = a+b$ and so $m+n = 0$. This can only be when $m = n = 0$ and so $x = y$.

Now suppose $x \leq_{\mathbb{Z}} y$ and $y \leq_{\mathbb{Z}} z$. Then there exist $m, n \in \mathbb{N}$ such that $x + [m,0] = y$ and $y +_{\mathbb{Z}} [n,0] = z$. This immediately gives $x + [m+n, 0] = z$ and so $x \leq_{\mathbb{Z}} z$.

For trichotomy, note that either $a + d \leq b + c$ or $b + c \leq a + d$ by trichotomy of $(\mathbb{N}, \leq)$. In the first case, $a + d + n = b + c$ for some $n \in \mathbb{N}$, so

$[a,b] +_{\mathbb{Z}} [n,0] = [c,d]$. Thus $x \leq_{\mathbb{Z}} y$. Similarly, in the second case, $y \leq x$. $\square$

Definition 1.7 (Ring)**.** A *ring* is a set S with two binary operations $+$ and $\cdot$ such that for all $a, b, c \in S$,

(R1) addition is associative,

(R2) addition is commutative,

(R3) there exists an additive identity 0,

(R4) there exists an additive inverse $-a$,

(R5) multiplication is associative,

(R6) there exists a multiplicative identity 1,

(R7) multiplication is distributive over addition (on both sides).

For a *commutative ring*, we require additionally that

(CR1) multiplication is commutative.

Note that inverses are unique, since if $a + b = 0$ and $a + b' = 0$, then $b = (b' + a) + b = b' + (a + b) = b'$.

Definition 1.8 (Ordered Ring)**.** An *ordered ring* is a ring S with a total order $\leq$ such that for all $a, b, c \in S$,

(OR1) $a \leq b$ implies $a + c \leq b + c$,

(OR2) $0 \leq a$ and $0 \leq b$ implies $0 \leq ab$.

Theorem 1.9.

- $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, \leq_{\mathbb{Z}})$ is an ordered (commutative) ring.
- The map $f = n \mapsto [n, 0]$ from $\mathbb{N}$ to $\mathbb{Z}$ is an injective map that respects $+$, $\cdot$ and $\leq$. That is, for all $n, m \in \mathbb{N}$,

  (i) $f(n + m) = f(n) +_{\mathbb{Z}} f(m)$,

  (ii) $f(nm) = f(n) \cdot_{\mathbb{Z}} f(m)$,

  (iii) $n \leq m \iff f(n) \leq_{\mathbb{Z}} f(m)$.

  In other words, f is an isomorphism onto a subset of $\mathbb{Z}$.

Proof. For the first part of the theorem, we check all commutative ring axioms. We omit the subscripts on $+$ and $\cdot$ for brevity.

(R1) Addition is associative:

$$\begin{aligned}\big([a,b]+[c,d]\big)+[e,f] &= [a+c,b+d]+[e,f]\\ &= [a+c+e,b+d+f]\\ &= [a,b]+[c+e,d+f]\\ &= [a,b]+\big([c,d]+[e,f]\big)\end{aligned}$$

(R2) Addition is commutative: immediate from commutativity of $+$ on $\mathbb{N}$.

(R3) Additive identity: $[a,b]+[0,0]=[a+0,b+0]=[a,b]$.

(R4) Additive inverse: $[a,b]+[b,a]=[a+b,b+a]=[0,0]$ since $a+b+0=b+a+0$.

(R5) Multiplication is associative:

$$\begin{aligned}\big([a,b]\cdot[c,d]\big)\cdot[e,f] &= [ac+bd,ad+bc]\cdot[e,f]\\ &= [ace+bde+adf+bcf,ade+bce+acf+bdf]\\ &= [a(ce+df)+b(cf+de),a(cf+de)+b(ce+df)]\\ &= [a,b]\cdot[ce+df,cf+de]\\ &= [a,b]\cdot\big([c,d]\cdot[e,f]\big)\end{aligned}$$

(R6) Multiplicative identity: $[a,b]\cdot[1,0]=[a,b]$.

(R7) Multiplication distributes over addition:

$$\begin{aligned}[a,b]\cdot\big([c,d]+[e,f]\big) &= [a,b]\cdot[c+e,d+f]\\ &= [ac+ae+bd+bf,ad+af+bc+be]\\ &= [ac+bd,ad+bc]+[ae+bf,af+be]\\ &= [a,b]\cdot[c,d]+[a,b]\cdot[e,f]\end{aligned}$$

Distributivity on the other side follows from commutativity proved below.

For commutativity of multiplication,

$$\begin{aligned}[a,b]\cdot[c,d] &= [ac+bd,ad+bc]\\ &= [ca+db,cb+da]\\ &= [c,d]\cdot[a,b]\end{aligned}$$

(OR1) follows immediately from the definition. For (OR2), suppose $0\leq x,y\in\mathbb{Z}$. Then $x=[n,0]$ and $y=[m,0]$ for some $n,m\in\mathbb{N}$. Thus $xy=[nm,0]$ and so $0\leq xy$.

The second part is again yawningly brute force.

(i) $f(n+m) = [n+m, 0] = [n, 0] + [m, 0] = f(n) +_{\mathbb{Z}} f(m)$.

(ii) $f(nm) = [nm, 0] = [n, 0] \cdot [m, 0] = f(n) \cdot_{\mathbb{Z}} f(m)$.

(iii) $n \leq m \iff \exists\, k \in \mathbb{N}(n + k = m) \iff \exists\, k \in \mathbb{N}\big([n, 0] + [k, 0] = [m, 0]\big) \iff f(n) \leq_{\mathbb{Z}} f(m)$. □

Thus, we may view $(\mathbb{N}, +, \cdot, \leq)$ as a subset of $(\mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, \leq_{\mathbb{Z}})$, denote $[n, 0]$ as n and drop $\mathbb{Z}$ in the subscript. We further define $-[a, b] := [b, a]$ and $z_1 - z_2 := z_1 + (-z_2)$.

Moreover, we have the following properties.

Proposition 1.10.

- There are no zero divisors in $\mathbb{Z}$. That is, for all $x, y \in \mathbb{Z}$, $xy = 0$ implies $x = 0$ or $y = 0$.
- The cancellation laws hold: for all $x, y, z \in \mathbb{Z}$, $x + y = x + z$ implies $y = z$, and $xy = xz$ implies $x = 0$ or $y = z$.
- (trichotomy) For all $z \in \mathbb{Z}$, $z = n$ or $z = -n$ for some $n \in \mathbb{N}$.

Proof.

- From trichotomy proven below, we have $x = n$ or $x = -n$ and $y = m$ or $y = -m$ for some $n, m \in \mathbb{N}$. In any case $xy = nm$ or $xy = -nm$. Since there are no zero divisors in $\mathbb{N}$, $xy = 0$ implies $n = 0$ or $m = 0$, which in turn implies $x = 0$ or $y = 0$.
- The first cancellation law follows from the fact that additive inverses exist. For the second, note that $xy = xz \iff x(y - z) = 0$ and invoke the fact that there are no zero divisors.

  Here we have also used that $-xz = x(-z)$, since $-\tilde{z} = -1 \cdot \tilde{z}$ for all $\tilde{z} \in \mathbb{Z}$, and multiplication is associative and commutative.
- Let $z = [a, b]$. From trichotomy of $\leq$ on $\mathbb{N}$ we know that either $a + n = b$ or $a = b + n$ for some $n \in \mathbb{N}$. (which $\mathbb{N}$?) That is, either $z = [0, n] = -n$, or $z = [n, 0] = n$.

□

1.4 The Rationals

We cannot solve $3x = 2$ in $\mathbb{Z}$.

Proof. Suppose $3x = 2$ for some $x = [a, b] \in \mathbb{Z}$. Then

$$\begin{aligned} 3x &= 2 \\ [3, 0] \cdot [a, b] &= [2, 0] \\ [3a, 3b] &= [2, 0] \\ 3a &= 3b + 2 \end{aligned}$$

What now? $\square$

We define $\mathbb{Z}^*$ to be $\mathbb{Z} \backslash \{0\}$ and define the relation R on $\mathbb{Z} \times \mathbb{Z}^*$ by $(a, b)R(c, d)$ if $ad = bc$. Then R is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^*$.

Definition 1.11. We define $\mathbb{Q}$ to be the set of equivalence classes of R, notated $\mathbb{Z} \times \mathbb{Z}^*/R$.

We define operations $+_{\mathbb{Q}}$ and $\cdot_{\mathbb{Q}}$ on $\mathbb{Q}$ by

$$\begin{aligned} [(a, b)] +_{\mathbb{Q}} [(c, d)] &:= [(ad + bc, bd)] \\ [(a, b)] \cdot_{\mathbb{Q}} [(c, d)] &:= [(ac, bd)] \end{aligned}$$

Since there are no zero divisors in $\mathbb{Z}$, $bd \neq 0$.

We define an order $\leq_{\mathbb{Q}}$ on $\mathbb{Q}$ by

$$[(a, b)] \leq_{\mathbb{Q}} [(c, d)] \iff (ad - bc)bd \leq 0.$$

We will again omit the parentheses in this section.

Proposition 1.12. The operations $+_{\mathbb{Q}}$, $\cdot_{\mathbb{Q}}$ and the relation $\leq_{\mathbb{Q}}$ are well-defined.

Proof. Suppose $[a, b] = [a', b']$ and $[c, d] = [c', d']$. Then

$$\begin{aligned} ab' &= a'b \\ cd' &= c'd \\ (ad + bc)(b'd') &= (a'd' + b'c')(bd) \\ [ad + bc, bd] &= [a'd' + b'c', b'd'] \end{aligned}$$

For multiplication,

$$\begin{aligned} (ac)(b'd') &= (a'c')(bd) \\ [ac, bd] &= [a'c', b'd'] \end{aligned}$$

For order,

$$\begin{aligned}
&(ad-bc)bd \leq 0\\
\implies &(a'c')(ad-bc)bd(a'c') \leq 0\\
\implies &(a'ac'd-a'bc'c)a'bc'd \leq 0\\
\implies &(a'acd'-ab'c'c)ab'cd' \leq 0\\
\implies &(ac)^2(a'd'-b'c')b'd' \leq 0\\
\implies &(a'd'-b'c')b'd' \leq 0
\end{aligned}$$

Similarly for the other direction. Thus $+_{\mathbb{Q}}$, $\cdot_{\mathbb{Q}}$ and $\leq_{\mathbb{Q}}$ are well-defined. □

Proposition 1.13. The relation $\leq_{\mathbb{Q}}$ is a total order on $\mathbb{Q}$.

Proof. **Transitivity:** Suppose $(ad-bc)bd \leq 0$ and $(cf-de)df \leq 0$. Then $(adf-bcf)bdf \leq 0$ and $(bcf-bde)bdf \leq 0$. Adding these gives $(adf-bde)bdf \leq 0$ and so $(af-be)bf \leq 0$.

Antisymmetry: Suppose $(ad-bc)bd \leq 0$ and $(cb-da)db \leq 0$. Then $(ad-bc)bd = 0$ which gives $ad = bc$ so $x = y$. □

Theorem 1.14.

- $(\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, \leq_{\mathbb{Q}})$ is an ordered field.
- The map $f = z \mapsto [z, 1]$ from $\mathbb{Z}$ to $\mathbb{Q}$ is an injective map that respects $+$, $\cdot$ and $\leq$. That is, for all $z_1, z_2 \in \mathbb{Z}$,

  (i) $f(z_1 + z_2) = f(z_1) +_{\mathbb{Q}} f(z_2)$,

  (ii) $f(z_1 z_2) = f(z_1) \cdot_{\mathbb{Q}} f(z_2)$,

  (iii) $z_1 \leq z_2 \iff f(z_1) \leq_{\mathbb{Q}} f(z_2)$.

  In other words, f is a commutative ring isomorphism into $\mathbb{Q}$.

Proof. For the first part, we check all ordered field axioms. We again omit the subscripts on $+$ and $\cdot$ for brevity. Numbering is from UMA101.

(F1) $+$ and $\cdot$ are commutative: immediate from commutativity of $+$ and $\cdot$ on $\mathbb{Z}$.

(F2) $+$ and $\cdot$ are associative:

$$\begin{aligned}\big([a,b]+[c,d]\big)+[e,f] &= [ad+bc,bd]+[e,f] \\ &= [(ad+bc)f+bde,bdf] \\ &= [adf+b(cf+de),bdf] \\ &= [a,b]+[cf+de,df] \\ &= [a,b]+\big([c,d]+[e,f]\big)\end{aligned}$$

Associativity of $\cdot$ is immediate from associativity on $\mathbb{Z}$.

(F3) Distributivity:

$$\begin{aligned}[a,b]\cdot\big([c,d]+[e,f]\big) &= [a,b]\cdot[cf+de,df] \\ &= [acf+ade,bdf] \\ &= [abcf+abde,b^2df] \qquad\qquad (b \text{ is nonzero}) \\ &= [(ac)(bf)+(bd)(ae),(bd)(bf)] \\ &= [ac,bd]+[ae,bf]\end{aligned}$$

(F4) Identities: $[0,1]\neq[1,1]$, $[a,b]+[0,1]=[a,b]$ and $[a,b]\cdot[1,1]=[a,b]$.

(F5) Additive inverse: $[a,b]+[-a,b]=[0,1]$.

(F6) Multiplicative inverse: $[a,b]\cdot[b,a]=[1,1]$ for $a\neq 0 \iff [a,b]\neq[0,1]$.

For the second part,

(i) $f(z_1+z_2)=[z_1+z_2,1]=[z_1,1]+[z_2,1]$.

(ii) $f(z_1z_2)=[z_1z_2,1]=[z_1,1]\cdot[z_2,1]$.

(iii) $f(z_1)\leq f(z_2) \iff (z_1-z_2)\leq 0 \iff z_1\leq z_2$. $\square$

We now introduce the division operation $/ : \mathbb{Q}\times\mathbb{Q}^*\to\mathbb{Q}$ by $a/b=\frac{a}{b}=ab^{-1}$.

Notation. Note that every rational number $x=[a,b]$ can be written as $x=a/b$. We thus largely drop the notation $[a,b]$ and write a/b instead.

We will now accept basic algebraic manipulations of rational numbers without justification.

Lecture 03: Wed 03 Jan '24

Definition 1.15 (Exponentiation)**.** The recursion principle guarantees the existence of $\mathrm{pow} : \mathbb{Z} \times \mathbb{N} \to \mathbb{N}$ such that for all $n, m \in \mathbb{N}$,

$$\begin{aligned} \mathrm{pow}(m, 0) &= 1 \\ \mathrm{pow}(m, n+1) &= m \cdot \mathrm{pow}(m, n) \end{aligned}$$

We extend this to $\mathrm{pow} : \mathbb{Q}^* \times \mathbb{Z} \to \mathbb{Q}$ as follows.

$$\mathrm{pow}\left(\frac{a}{b}, m\right) := \begin{cases} a^m/b^m & \text{if } m \in \mathbb{N} \\ b^m/a^m & \text{if } -m \in \mathbb{N} \end{cases}$$

We write z^n to denote $\mathrm{pow}(z, n)$.

Remarks. Note that we have defined 0^0 to be 1, but we don't really care.

Proposition 1.16. Expoentiation is well-defined.

Proof. Let $a/b = \tilde{a}/\tilde{b} \in \mathbb{Q}$. That is, $a\tilde{b} = b\tilde{a} \in \mathbb{Z}$. For $m \in \mathbb{N}$, thus $a^m\tilde{b}^m = b^m\tilde{a}^m$ (easily proved by induction).

Similarly if $-m \in \mathbb{N}$. □

Theorem 1.17. There exists no $x \in \mathbb{Q}$ such that $x^2 = 2$.

We first make note of the following lemma.

Lemma 1.18. Let $x \in \mathbb{Q}$. Then there exists $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ such that $x = p/q$.

In particular, if $x > 0$, then $x = p/q$ for some $p \in \mathbb{N}$, $q \in \mathbb{N}^*$.

Proof. Let $x = a/b$. If $b \in \mathbb{N}$, we are done. Otherwise, $x = -a/-b$ and $-b \in \mathbb{N}$. □

We will make use of the well-ordered property of $(\mathbb{N}, \leq)$ proved below in theorem 1.19.

Proof of theorem 1.17. Suppose there exists such an x. By the field properties, $(-x)^2 = x^2$. Thus we may assume $x \geq 0$. Let $x = p/q$ for some $q \in \mathbb{N}^*$. Since $x \geq 0$, we have $p \geq 0 \iff p \in \mathbb{N}$.

Let $A = \{q \in \mathbb{N}^* \mid x = p/q \text{ for some } p \in \mathbb{N}\}$. A is non-empty.

By the well-ordering principle, A has a least element q_0. Let $p_0 \in \mathbb{N}$ such that $x = p_0/q_0$.

We know that $1 < x < 2$ [why? because $(\cdot)^2$ is an increasing function on positive reals (why? difference of squares)] and so $0 < p_0 - q_0 < q_0$. Now

$$\begin{aligned} \frac{2q_0 - p_0}{p_0 - q_0} &= \frac{2-x}{x-1} \\ &= \frac{(2-x)(x+1)}{x^2-1} \\ &= 2x + 2 - x^2 - x \\ &= x, \end{aligned}$$

in contradiction to the minimality of q_0. □

Theorem 1.19 (Well-ordering principle)**.** Every non-empty subset of $\mathbb{N}$ has a least element.

Proof. Let $S \subseteq \mathbb{N}$ be non-empty. We define $P(n)$ to be "if $n \in S$, then S has a least element". Clearly $P(0)$ holds.

Suppose $P(k)$ holds for all $k \leq n \in \mathbb{N}$.
If $n+1 \notin S$, $P(n+1)$ holds vacuously.
If $\exists\, m \in S (m < n+1)$, then $P(n+1)$ holds by virtue of $P(m)$.
Otherwise $n+1 \in S$ and $\forall\, m \in S (n+1 \leq m)$, so that $n+1$ is the least element of S.

In any case, $P(n+1)$ holds. □

Theorem 1.20. Let

$$\begin{aligned} A &= \left\{ x \in \mathbb{Q} \mid x^2 < 2 \right\} \\ B &= \left\{ x \in \mathbb{Q} \mid x^2 > 2, x > 0 \right\} \end{aligned}$$

Then A has no largest element and B has no smallest element.

Proof. Let $a \in A$. $a > -2$ since otherwise $a^2 \geq 4$. Let $c = a + \frac{2-a^2}{2+a}$. Clearly

$c > a$. Now

$$\begin{aligned} c &= \frac{2a+2}{2+a} \\ c^2 &= \frac{4a^2+8a+4}{4+4a+a^2} \\ c^2-2 &= \frac{2a^2-4}{(2+a)^2} < 0 \end{aligned}$$

Thus $c \in A$.

For B, let $c = b + \frac{2-b^2}{2+b} = \frac{2b+2}{2+b}$. Clearly $0 < c < b$ and $c^2 - 2 = \frac{2b^2-4}{(2+b)^2} > 0$. Thus $c \in B$. □

1.5 Ordered Fields with LUB

(Recall from UMA101 Lecture 6) Given an ordered set $(X, \leq)$, a subset $S \subseteq X$ is said to be *bounded above* (resp. below) if there exists $x \in X$ such that for all $s \in S$, $s \leq x$ (resp. $x \leq s$), and any such x is called an *upper* (resp. lower) *bound* of S.

A (The) *supremum* or least upper bound of S is an element $x \in X$ such that x is an upper bound of S and for all upper bounds y of S, $x \leq y$. Similarly, infimum or greatest lower bound.

$(X, \leq)$ is said to have the least upper bound property if every non-empty bounded above subset of X admits a supremum.

Proposition 1.21. $(\mathbb{Q}, \leq)$ does not have the least upper bound property.

Proof. From theorem 1.20, we know that A has no largest element and B has no smallest element.

Let s be a supremum of A. Since there is no largest element in A, $s \notin A$. From theorem 1.17, we know that $s^2 \neq 2$. Thus by trichotomy, $s^2 > 2$ and so $s \in B$. But then there is an $s' \in B$ which is less than s but also an upper bound of A. This is a contradiction. □

Theorem 1.22. Every ordered field F "contains" $\mathbb{Q}$, *i.e.*, there exists an injective map $f : \mathbb{Q} \to F$ that respects $+$, $\cdot$ and $\leq$.

We will notate this statement as $\mathbb{Q} \subseteq F$.

Proof. Let $f : \mathbb{Z} \to F$ be defined as

$$f(n) = \begin{cases} 0_F & \text{if } n = 0 \\ \underbrace{1_F + \cdots + 1_F}_{n \text{ times}} & \text{if } n > 0 \\ \underbrace{(-1_F) + \cdots + (-1_F)}_{m \text{ times}} & \text{if } n = -m, m > 0 \end{cases}$$

Note that $f(-n) = -f(n)$ for all $n \in \mathbb{N}$. Let us show that $f(n+m) = f(n) + f(m)$ for all $n, m \in \mathbb{Z}$.

Case 1: $n = 0$ or $m = 0$. Immediate.

Case 2: $n > 0$ and $m > 0$. Then

$$\begin{aligned} f(n+m) &= \underbrace{1_F + \cdots + 1_F}_{n+m \text{ times}} \\ &= \underbrace{1_F + \cdots + 1_F}_{n \text{ times}} + \underbrace{1_F + \cdots + 1_F}_{m \text{ times}} \\ &= f(n) + f(m) \end{aligned}$$

Case 3: $n < 0$ and $m < 0$. Then $f(n+m) = -f((-n)+(-m)) = -(f(-n) + f(-m)) = f(n) + f(m)$.

Case 4: $nm < 0$. WLOG, let $m < 0 < n$. Suppose $0 < n + m$. Then $f(n+m) + f(-m) = f(n+m-m) = f(n)$ from case 2. Now suppose $n + m < 0$. Then $f(n) + f(-n-m) = f(n-n-m) = -f(m)$ from case 3. In either case, $f(n+m) = f(n) + f(m)$.

Now consider $f(nm)$. If $nm = 0$, then $f(nm) = 0_F = f(n)f(m)$. If $0 < n, m$, then

$$\begin{aligned} f(nm) &= \overbrace{1_F + \cdots + 1_F}^{nm \text{ times}} \\ &= \underbrace{\overbrace{(1_F + \cdots + 1_F)}^{n \text{ times}} + \cdots + \overbrace{(1_F + \cdots + 1_F)}^{n \text{ times}}}_{m \text{ times}} \\ &= \underbrace{(1_F + \cdots + 1_F)}_{n \text{ times}} \cdot \underbrace{(1_F + \cdots + 1_F)}_{m \text{ times}} \\ &= f(n)f(m) \end{aligned}$$

If either of n, m is negative, then we take the negative sign out and use the above case.

Thus f respects $+$ and $\cdot$.

Suppose that $m < n$. Then $f(n) - f(m) = f(n) + f(-m) = f(n-m) =$

$(n-m)1_F$ (where $z1_F$ is notation for 1_F added z times). $n-m$ is positive, but 1_F added to itself a positive number of times must be positive. This is because $0_F < 1_F$ (UMA101) and so $k1_F < (k+1)1_F$ for all $k \in \mathbb{N}^+$. Induction gives $0_F < k1_F$ for all $k \in \mathbb{N}^+$. Thus $f(m) < f(n)$ and so f respects $<$ (and hence $\leq$).

Finally, injectivity of f follows from order preservation. $\square$