

1. REAL & COMPLEX NUMBERS

• Inadequacies of rationals:

Th^m 1.1: There is no $p \in \mathbb{Q}$ s.t. $p^2 = 2$.

Pf: Sps there is a $p = a/b$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $(a, b) = 1$
s.t. $p^2 = 2$. Then no common factor

$$a^2 = 2b^2$$

Since 2 is a prime, $2 \mid a^2$ (2 divides a^2)

$\Rightarrow 2 \mid a$ let $a = 2m$. Then

$$b^2 = 2m^2$$

Again $2 \mid b^2$, and hence $2 \mid b$. So 2 is a common factor between a & b . Contradiction! \square

So algebraically there is no rational solution to $x^2 - 2 = 0$. Analytically the problem is that \mathbb{Q} has "gaps". That is we have

Th^m 1.2 The set

$$A = \{p \in \mathbb{Q} \mid p^2 \leq 2\}$$

has no largest element.

Pf: Sps q is such a largest element. Then by

Th^m 1.1, $q^2 < 2$. One

For N a big rational \neq , consider

$$z = q + \frac{1}{N}$$

Then $2 - z^2 = 2 - q^2 - \frac{1}{N} \left(\frac{1}{N} + 2q \right)$

(Choose N big enough s.t. $\frac{1}{N} \left(\frac{1}{N} + 2q \right) < 2 - q^2$)

A way to do this is the foll. We firstly pick $N \geq 1$. Then

$$\frac{1}{N} \left(\frac{1}{N} + 2q \right) < \frac{1 + 2q}{N}$$

So if we let $N = (1 + 2q) / (2 - q^2) \in \mathbb{Q}$, then since $(q+1)^2 > 2$, we can check $N \geq 1$. Moreover,

then $\frac{1}{N} \left(\frac{1}{N} + 2q \right) < \frac{1 + 2q}{N} = 2 - q^2$

In any case, we have found an $z = q + \frac{1}{N} \in \mathbb{Q}$, $z > q$ but $z^2 < 2$. So q cannot be the largest element of A . Contradiction!

Rk: When we construct \mathbb{R} , " A " will "correspond" to the $\# \sqrt{2}$.

• Construction of reals \mathbb{R} We need \mathbb{R} to have 3 properties.

(1) $\mathbb{Q} \subseteq \mathbb{R}$ More precisely an injection $i: \mathbb{Q} \rightarrow \mathbb{R}$

(2) Order on \mathbb{R} which extends the order on \mathbb{Q} .

(3) Addition⁽⁺⁾, Multiplication^(\cdot) extending + and \cdot on \mathbb{Q}

Defⁿ: A cut is a subset $\alpha \subseteq \mathbb{Q}$ s.t.

(1) $\alpha \neq \emptyset$, $\alpha \neq \mathbb{Q}$

(2) $p \in \alpha$, $q \in \mathbb{Q}$, $q < p \Rightarrow q \in \alpha$



(3) $p \in \alpha \Rightarrow \exists r \in \alpha$ s.t. $p < r$. i.e. α has no largest element.

Example $\alpha = \{p \in \mathbb{Q} \mid p < 0\} \cup \{p \in \mathbb{Q} \mid p^2 < 2\}$
 $= \{p \in \mathbb{Q} \mid p < 0 \underline{or} p^2 < 2\}$

is a cut.

Defⁿ: Define the set of reals \mathbb{R} by

$$\mathbb{R} := \{ \alpha \subseteq \mathbb{Q} \mid \alpha \text{ is a cut} \}$$

Th^m 1-3 The function $i: \mathbb{Q} \rightarrow \mathbb{R}$
 $p \mapsto \alpha_p := \{ q \in \mathbb{Q} \mid q < p \}$

is well defined and injection.

Pf 1) Well defined: We need to show $\alpha_p \in \mathbb{R} \forall p \in \mathbb{Q}$

Properties (1) & (2) are trivial. For (3), s.p.s. z is the largest element of α , i.e. $z \in \alpha$ and $q \leq z \forall q \in \alpha$. Then consider

$$z' = \frac{z+p}{2}$$

Since $z < p$, $z < z' < p$. So $z' \in \alpha$, but $z' > z$, contradicting that z is the largest element.

2) Injective. If not, then $\exists p_1, p_2 \in \mathbb{Q}$ s.t.
 $\alpha_{p_1} = \alpha_{p_2}$. S.p.s. $p_1 < p_2$. Then $p_1 \in \alpha_{p_2}$. But $p_1 \notin \alpha_{p_1}$. So $\alpha_{p_1} \neq \alpha_{p_2}$. Contradiction. Similarly, if $p_2 < p_1$, then $\alpha_{p_1} \neq \alpha_{p_2}$. So $p_1 = p_2$.

\mathbb{R} as an ordered set

Defⁿ: Let S be any set. An order on S is a relation $<$ ^(less than) with the foll. properties:

$$(1) x, y \in S \Rightarrow x < y \text{ or } x = y \text{ or } y < x$$

$$(2) x, y, z \in S, x < y, y < z \Rightarrow x < z$$

We then call S , an ordered set.

Rk: If $x < y$, we sometimes also write $y > x$.

We denote $x \leq y$ if $x < y$ or $x = y$.

Defⁿ: Sp. S is ordered. We say $E \subseteq S$ is bounded above if $\exists \beta \in S$ s.t. $x \leq \beta \forall x \in E$, and call β an upper bound ^(u.b.) on E .

Similarly we can define bounded below and lower bounds.

Example: \mathbb{Q} with the usual order. $\left(\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow ad \leq bc\right)$

$E = \{p \mid p^2 < 2\}$ is bounded above by 2 and below by -2 while \mathbb{N} is only bounded below.

Defⁿ: Sps S is an ordered set and $E \subseteq S$ is bounded above. Sps $\exists \alpha \in S$ s.t

(1) α is an u.b for E .

(2) If γ is another u.b $\Rightarrow \gamma \geq \alpha$.

We then say that α is the least upper bound (l.u.b) on E or supremum of E ,

$$\alpha = \sup E$$

Similarly if E is bounded below we can define greatest lower bound (g.l.b) written as $\inf E$ or infimum of E .

Rk: If $\alpha = \sup E$, we might not have $\alpha \in E$.

For instance

$$E = \{q \in \mathbb{Q} \mid q < 0\} \subseteq \mathbb{Q}$$

Then $\sup E = 0$, but $0 \notin E$.

Defⁿ: An ordered set S is said to have the least upper bound property if every $E \subseteq S$, $E \neq \emptyset$, bounded above has an l.u.b.

Rk: One can similarly define S having the g.l.b property. It turns out that S has l.u.b property $\iff S$ has g.l.b property.

Thm^{1.4} For $\alpha, \beta \in \mathbb{R}$ if we define $\alpha < \beta$ if $\alpha \not\subseteq \beta$, then \mathbb{R} is an ordered set with l.u.b property.

Pf: (i) $(\mathbb{R}, <)$ is an ordered set: We first show that if $\alpha \neq \beta$, then $\alpha < \beta$ or $\beta < \alpha$. To see this, since $\alpha \neq \beta$, $\exists p \in \alpha, p \notin \beta$ OR $\exists p \in \beta, p \notin \alpha$.

In the first case we claim:

Claim If $\exists p \in \alpha, p \notin \beta$, then $\beta \subset \alpha$. To see,

thm, let $q \in \beta$. Then by (ii) of cuts if $q > p$, $\Rightarrow p \in \beta$. Contradiction. So $q \leq p$. But then, again by (ii), $q \in \alpha$. So $\beta \subset \alpha$.

In the second case one can show $\alpha \subset \beta$.

So any two $\alpha, \beta \in \mathbb{R}$ satisfy $\alpha < \beta$, $\alpha = \beta$ or

$\beta < \alpha$. Also clearly $\alpha < \beta, \beta < \gamma \Rightarrow \alpha < \beta, \beta < \gamma$

$\Rightarrow \alpha < \gamma \Rightarrow \alpha < \gamma$. So $(\mathbb{R}, <)$ is an ordered set.

(2) $(\mathbb{R}, <)$ has the l.u.b prop. Let $E \subset \mathbb{R}$

bounded above. Define

$$\alpha = \{p \in \mathbb{Q} \mid p \in \beta \text{ for some } \beta \in E\}.$$

i.e. α is the union of all cuts in E .

Claim: $\alpha \in \mathbb{R}$ and $\alpha = \sup E$.

Pf: Firstly, $\alpha \neq \emptyset$ since E is non-empty.

Also, since E is bounded above, $\exists r \in \mathbb{R}$ s.t. $\beta < r \ \forall \beta \in E \Rightarrow \alpha \subseteq r \Rightarrow \alpha \neq \mathbb{Q}$

Since $r \neq \mathbb{Q}$ (being a cut). Now if $p \in \alpha$ and $q < p$, then $\exists \beta \in E$ s.t. $p \in \beta$. Since β is a cut, and $q < p \Rightarrow q \in \beta \Rightarrow q \in \alpha$.

So α satisfies (ii) of defⁿ of cut

As for (iii) if $p \in \alpha$, then $p \in \beta$ for some $\beta \in E$

Since β is a cut, by (iii) $\exists z \in \beta$, s.t. $p < z$.

$\Rightarrow \exists z \in \alpha$ s.t. $p < z$. So α has no largest element. So $\boxed{\alpha \text{ is a cut, i.e. } \alpha \in \mathbb{R}}$

By defⁿ of α , if $\beta \in E$ then $\beta \subset \alpha$ i.e.

$\beta < \alpha$. So α is an u.b on E .

If r is an upper bound, then $\beta < r \ \forall \beta \in E$

$\Rightarrow \alpha \subset r \Rightarrow \alpha \leq r$. So α is the least upper bound. Done!

• Arithmetic in \mathbb{R}

Defⁿ 1) Addition (+). For $\alpha, \beta \in \mathbb{R}$, define

$$\alpha + \beta := \{p \in \mathbb{Q} \mid p = r + s, r \in \alpha, s \in \beta\}$$

$$0 = \{p \in \mathbb{Q} \mid p < 0\}$$

2) Multiplication (\cdot). For $\alpha, \beta > 0$ define

$$\alpha \cdot \beta = \{p \in \mathbb{Q} \mid p \leq rs, r \in \alpha, s \in \beta, r, s > 0\}$$

$$1 = \{p \in \mathbb{Q} \mid p < 0\}$$

In general.

$$\alpha \cdot \beta = \begin{cases} -(-\alpha) \cdot (\beta) & \alpha < 0, \beta > 0 \\ -(\alpha) \cdot (-\beta) & \beta < 0, \alpha > 0 \\ (-\alpha) \cdot (-\beta) & \alpha, \beta < 0 \end{cases}$$

where for $\alpha \in \mathbb{R}$, define

$$-\alpha := \{p \in \mathbb{Q} \mid \exists r, s, t \text{ } -p - r \notin \alpha\}$$

Check: $\alpha + (-\alpha) = 0$

Thm 1.5: $(\mathbb{R}, +, \cdot)$ satisfies the field axioms.

A1: If $\alpha, \beta \in \mathbb{R} \Rightarrow \alpha + \beta, \alpha \cdot \beta \in \mathbb{R}$.

A2: (Commutativity) $\alpha + \beta = \beta + \alpha$
 $\alpha \cdot \beta = \beta \cdot \alpha$

A3 (Associativity) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$
 $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

A4 (Identity element) $\alpha + 0 = \alpha \quad \forall \alpha \in \mathbb{R}$
 $\alpha \cdot 1 = \alpha \quad \forall \alpha \in \mathbb{R}$

A5 (Inverses) $\forall \alpha \in \mathbb{R}, \alpha + (-\alpha) = 0$
 $\forall \alpha \in \mathbb{R}, \alpha \neq 0, \exists \beta \in \mathbb{R}$ s.t.
 $\alpha \cdot \beta = 1$. We write $\beta = 1/\alpha$.

A6 (Distributive) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$

Moreover $(\mathbb{R}, <, +, \cdot)$ is an ordered field.

i.e.

OF1: $\beta < \gamma \Rightarrow \alpha + \beta < \alpha + \gamma$

OF2: $\alpha, \beta > 0 \Rightarrow \alpha \cdot \beta > 0$

Pf: See Appendix of Ch. 1 in Rudin!

Rk: From Th^m 1.5, one can derive most of the basic arithmetic properties of reals. See Props 1.14, 1.15, 1.16 and 1.18 in Rudin.

• Two Important Consequences.

Th^m 1.6. (a) (Archimedean prop.) If $x, y \in \mathbb{R}$, $x > 0$, then $\exists n \in \mathbb{N}$ s.t.
 $nx > y$.

(b) (Density of \mathbb{Q}) If $x, y \in \mathbb{R}$, $x < y$, $\exists p \in \mathbb{Q}$ s.t. $x < p < y$.

Pf: (a) let $A = \{nx \mid n \in \mathbb{N}\}$. If (a) is not true $\Rightarrow y$ is an u.b. for A . Since \mathbb{R} has l.u.b. property, let $\alpha = \sup A$. $x > 0 \Rightarrow \alpha - x < \alpha$. So $\alpha - x$ is not u.b. for A (or else α cannot be l.u.b.). So $\exists m \in \mathbb{N}$ s.t. $\alpha - x < mx$. Then $\alpha < (1+m)x$.

Contradiction!

(b) If $x, y \in \mathbb{R}$, $x < y$, since $x \neq y$, $\exists p \in \mathbb{Q}$, $p \in y$, $p \notin x$ (thinking of x and y as cuts). But then the cut α_p satisfies
 $x \subseteq \alpha_p \subseteq y$ & so $x < p < y$.

Thm 1.7: For all $x \in \mathbb{R}$, $x > 0$ and $\forall n \in \mathbb{N}$,

\exists unique $y > 0$, $y \in \mathbb{R}$ s.t. $y^n = x$.

Pf: Uniqueness. If $y_1 < y_2 \implies y_1^n < y_2^n$
i.e. $y_1^n \neq y_2^n$.

Existence: let $E = \{t \in \mathbb{R} \mid t^n < x\}$.

Claim 1: $t = x/(1+x) \in E$

Pf: $t < 1 \implies t^n < t < x \implies t \in E$
 $t < x$

Claim 2: $1+x$ is an u.b. for E

Pf: If $t > 1+x$, then $t > 1 \implies t^n > t > x$
 $t > x$.

So $t \notin E$. So $\forall t \in E$, $t \leq 1+x$.

From Claim 1 & Claim 2, $E \neq \emptyset$ & E is bounded above. Since \mathbb{R} has l.u.b. prop.

$\implies \exists y = \sup E$

Claim 3: $y^n = x$.

Pf: Sps $y^n < x$. For some small h , $0 < h < 1$,

let $z = y + h$, since $y < z < y + 1$

$$z^n - y^n = h(z^{n-1} + z^{n-2}y + \dots + y^{n-1}) < nhz^{n-1} < nh(y+1)^{n-1}$$

if we let $h = \min\left(1^n, \frac{x - y^n}{n(1+y)^{n-1}}\right) < 1$

$$z^n - y^n < x - y^n \Rightarrow z^n < x. \text{ So } z \in E$$

Also $z > y$. So y cannot be sup.

Contradiction.

If $y^n > x$, let $w = y - k$, for some $0 < k < y$.
which we pick later.

Claim: For a suitable choice of k , $y - k$ is an upper bound for E contradicting that y is the least upper bound.

Pf: Let $t \geq y - k$, then

$$y^n - t^n \leq y^n - (y - k)^n = k(y^{n-1} + y^{n-2}(y - k) + \dots + (y - k)^{n-1})$$

$$< k \cdot n \cdot y^{n-1}$$

Sp s $k = \frac{y^n - x}{n \cdot y^{n-1}}$, then by assumption $k > 0$

Also $k < y$. since $y^n - x < n \cdot y^n$ (remember $x > 0$).

With this k

$$y^n - t^n < y^n - x \text{ or } t^n > x, \text{ so } t \notin E.$$

$\Rightarrow y - k$ is an u.b on E . proving the claim

& the theorem!

• Decimal representation. The representation of \mathbb{R} as cuts is useful to prove theorems, but is cumbersome to use, especially in doing arithmetic. A more convenient form is the Indo-Arabic numerals.

Let $x \in \mathbb{R}$. For simplicity, suppose $x > 0$.

Let $d_0 > 0$ be the largest natural number

s.t. $d_0 \leq x$.

Then let d_1 be the largest natural number s.t.

$$d_0 + \frac{d_1}{10} \leq x.$$

Having chosen d_0, \dots, d_{k-1} , let d_k be the largest natural # s.t.

$$d_0 + \frac{d_1}{10} + \dots + \frac{d_{k-1}}{10^{k-1}} + \frac{d_k}{10^k} \leq x.$$

d_0, \dots, d_k, \dots exist thanks to the Archimedean property. Note $d_k \leq 9 \quad \forall k$. Let

$$E = \left\{ d_0, d_0 + \frac{d_1}{10}, \dots, d_0 + \frac{d_1}{10} + \dots + \frac{d_k}{10^k}, \dots \right\}.$$

Then E is bounded above by x , is non-empty and so has a l.u.b

Claim: $x = \sup E$.

Pf: Since x is an upper bound, clearly
 $x \geq \sup E$ Sp. $x > \sup E$.

$\exists k \in \mathbb{N}$ s.t. $x - \sup E > \frac{1}{10^k}$.

or $x > \sup E + \frac{1}{10^k}$.

But $d_0 + \frac{d_1}{10} + \dots + \frac{d_k}{10^k} < \sup E$.

$\Rightarrow d_0 + \frac{d_1}{10} + \dots + \frac{d_k}{10^k} + \frac{1}{10^k} < x$.

But d_k was the largest integer s.t.

$$d_0 + \frac{d_1}{10} + \dots + \frac{d_k}{10^k} \leq x$$

Contradiction! since d_{k+1} would also work.

• Complex numbers.

Defⁿ: A complex number is an ordered pair (a, b) where $a \in \mathbb{R}$, $b \in \mathbb{R}$. Ordered means simply that (a, b) & (b, a) are distinct complex numbers if $a \neq b$. Denote the set of complex numbers by \mathbb{C} .

Defⁿ Addition is defined as

$$(a, b) + (c, d) = (a+c, b+d)$$

Additive identity is $(0, 0)$.

Defⁿ: Define 'i' to be the number $(0, 1) \in \mathbb{C}$.

Defⁿ: For multiplication if $t \in \mathbb{R}$ define

$$t(a, b) = (ta, tb)$$

Define $i^2 = -1$; and extend s.t the distributive property holds.

Lemma 1.8 $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$ and

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc)$$

Pf: Easy exercise!

Th^m 1.9: $(\mathbb{C}, +, \cdot)$ is a field i.e \mathbb{C} with $+$, \cdot satisfies the axioms A1 - A6 in Th^m 1.5.

Defⁿ: 1) For a $z \in \mathbb{C}$, if $z = a + ib$, define the conjugate $\bar{z} = a - ib$.

2) Define the modulus or absolute value by

$$|z| = \sqrt{a^2 + b^2}$$

3) Define real & imaginary parts by

$$\operatorname{Re}(z) = a, \quad \operatorname{Im}(z) = b.$$

Lemma 1.10 1) $\operatorname{Re}(z) = \frac{z + \bar{z}}{2}, \quad \operatorname{Im}(z) = \frac{z - \bar{z}}{2i}$

2) $|z|^2 = z \cdot \bar{z}$

3) $|z| > 0$, and $|\cdot|$ satisfies

$$|z + w| \leq |z| + |w|.$$

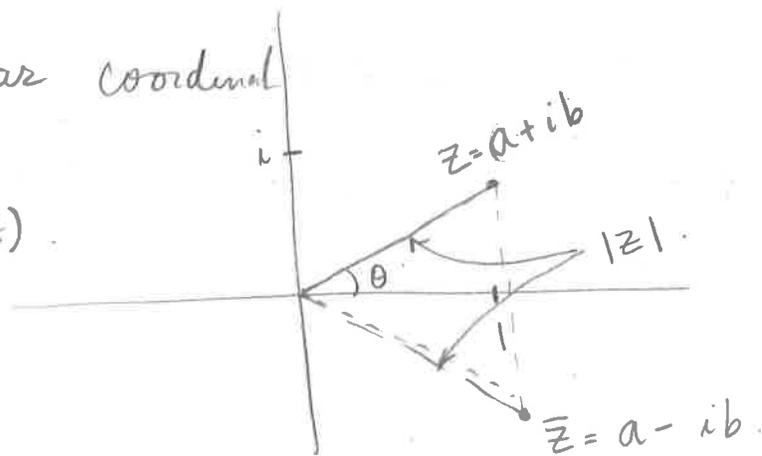
Geometric representation $z = (a, b)$ can be thought of as a point in the plane

Also use polar coordinates

$$z = r e^{i\theta}$$

θ is called $\arg(z)$.

$$r = |z|.$$



• Euclidean Spaces

Defⁿ: Define the n -dimensional Euclidean spaces by

$$\mathbb{R}^n = \{ \vec{x} = (x_1, \dots, x_n) \mid x_k \in \mathbb{R} \forall k \}$$

As sets $\mathbb{R}^2 = \mathbb{C}$.

We can define addition by

$$\vec{x} + \vec{y} = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$$

$$\vec{0} = (0, 0, \dots, 0)$$

This makes \mathbb{R}^n into a vector space. It is NOT a field unless $n=1, 2$ since there is no natural product that satisfies field axioms. Note that in \mathbb{R}^3 we do have cross prod., but this is not commutative.

Defⁿ: For $\vec{x} \in \mathbb{R}^n$, define ($\vec{x} = (x_1, \dots, x_n)$)

$$|\vec{x}| = \sqrt{x_1^2 + \dots + x_n^2}$$

This is called the absolute value or the "distance of \vec{x} from origin $\vec{0}$ ".

Th^m 1.11: (Triangle inequality) For $\vec{x}, \vec{y} \in \mathbb{R}^n$,

$$|\vec{x} - \vec{y}| \leq |\vec{x}| + |\vec{y}|$$