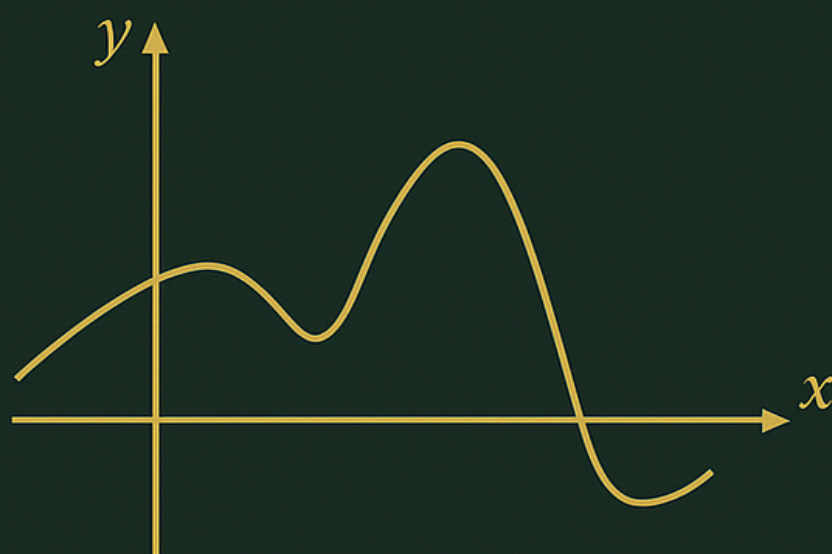


# REAL ANALYSIS

A SELF-TAUGHT APPROACH



Luis Vasquez

# REAL ANALYSIS

A Self-Taught Approach

Luis Vasquez

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Sources . . . . .	3
1.2	Purpose . . . . .	3
<b>2</b>	<b>Base knowledge</b>	<b>4</b>
2.1	What is a Field . . . . .	4
2.2	Formal definition . . . . .	6
2.1	Field . . . . .	6
2.1	Distributive law . . . . .	6
2.1	Zero uniqueness . . . . .	6
2.3	Order . . . . .	8
2.2	Ordered sets . . . . .	8
2.3	Ordered fields . . . . .	8
2.4	Completeness . . . . .	9
2.4	Bounds . . . . .	9
2.7	Least Upper Bound . . . . .	9
2.8	Greatest Lower Bound . . . . .	10
2.3	Uniqueness of Supremum . . . . .	10
2.9	Complete Ordered Field . . . . .	11
2.4	Least Upper Bound Principle . . . . .	13
2.5	Archimedean property . . . . .	13
<b>3</b>	<b><math>\mathbb{R}</math> as the complete ordered field</b>	<b>16</b>
3.1	$\mathbb{F}$ is $\mathbb{R}$ . . . . .	16
3.1.1	Isomorphism . . . . .	16
3.1	Field homomorphism . . . . .	16
3.2	Field isomorphism . . . . .	16
3.1	Injectivity by order preservation . . . . .	17
3.2	Surjectivity by construction . . . . .	17
3.1.2	Sets construction . . . . .	18

# 1 Introduction

## 1.1 Sources

The following notes are taken from the compilation of a few sources

- Zorich, V. A. (2004). Mathematical analysis I (R. Cooke, Trans.). Springer.
- MIT 18.100B Real Analysis, Spring 2025, available at the MIT OCW youtube channel

## 1.2 Purpose

This notes are taken in a way that is easy to understand math. No obscure proof or incomplete idea will be included, avoiding partial understanding of a certain topic. It also covers the need of having an easy-to-follow approach to *Real Analysis*, making it possible to read this through to revisit known topics without the need of looking at other sources and rabbit-hole-ing into old books with russian last names on its cover. Since I will also be studying the course while taking this notes, the document as a whole will be written by hand without any AI slob nor blind copy/pasting, and since English is not my native language, typos may happen.

*When I say **we**, it means you (the reader) and I. When I say **I**, responsibility only lies on me.*

## 2 Base knowledge

### 2.1 What is a Field

*“We can verify that a set is a field by checking that multiplication is a well-defined operation, i.e., it is independent of the representative.”*

For example, for arbitrary rational numbers  $Q$ :

$$\frac{m_1}{n_1} \times \frac{p_1}{q_1}$$

And evaluate an equivalent expression with different representatives of the same numbers:

$$\frac{m_2}{n_2} \times \frac{p_2}{q_2}$$

Given that:

$$\frac{m_1}{n_1} = \frac{m_2}{n_2} \quad \text{and} \quad \frac{p_1}{q_1} = \frac{p_2}{q_2}$$

We want to verify that both multiplication results are the same. To review this, we start from the tautology (intuitive truth):

$$\frac{m_1}{n_1} = \frac{m_2}{n_2} \iff m_1 \times n_2 = m_2 \times n_1 \tag{A}$$

$$\frac{p_1}{q_1} = \frac{p_2}{q_2} \iff p_1 \times q_2 = p_2 \times q_1 \tag{B}$$

Then, operating the multiplication using both representatives:

$$\begin{aligned} \frac{m_1}{n_1} \times \frac{p_1}{q_1} &= \frac{m_1 \cdot p_1}{n_1 \cdot q_1} \\ \frac{m_2}{n_2} \times \frac{p_2}{q_2} &= \frac{m_2 \cdot p_2}{n_2 \cdot q_2} \end{aligned}$$

Conveniently, we want to form  $m_1 \times n_2$  to use the first ground truth:

$$\begin{aligned} \frac{m_1}{n_1} \times \frac{p_1}{q_1} \times n_2 &= \frac{m_1 \cdot n_2 \cdot p_1}{n_1 \cdot q_1} \\ &= \frac{m_2 \cdot n_1 \cdot p_1}{n_1 \cdot q_1} \quad (\text{replacing using A}) \\ &= \frac{m_2 \cdot p_1}{q_1} \quad (\text{simplifying } n_1) \end{aligned}$$

Applying the same logic for  $p_1 \times q_2$  to use the second ground truth:

$$\begin{aligned} \frac{m_1}{n_1} \times \frac{p_1}{q_1} \times n_2 \times q_2 &= \frac{m_2 \cdot p_1 \cdot q_2}{q_1} \\ &= \frac{m_2 \cdot p_2 \cdot q_1}{q_1} \quad (\text{replacing using B}) \\ &= m_2 \cdot p_2 \quad (\text{simplifying } q_1) \end{aligned}$$

Finally, rearranging:

$$\begin{aligned}\frac{m_1}{n_1} \times \frac{p_1}{q_1} \times n_2 \times q_2 &= m_2 \cdot p_2 \\ \frac{m_1}{n_1} \times \frac{p_1}{q_1} &= \frac{m_2 \cdot p_2}{n_2 \cdot q_2} \\ \frac{m_1}{n_1} \times \frac{p_1}{q_1} &= \frac{m_2}{n_2} \times \frac{p_2}{q_2} \quad \square\end{aligned}$$

This is not a rigorous demonstration, but gives us a first step to go from the intuition of a solution (particularly for  $\mathbb{Q}$ ) to a more formal procedure based on the real definition of a field.

## 2.2 Formal definition

<b>Definition</b>	A <b>field</b> $\mathbb{F}$ is a set with two operations: addition ( $\oplus$ ) and multiplication ( $\otimes$ ), with the following properties:
Field	
2.1	<ul style="list-style-type: none"> <li>• <math>x, y \in \mathbb{F} \implies x \oplus y \in \mathbb{F}</math></li> <li>• <math>x, y \in \mathbb{F} \implies x \oplus y = y \oplus x</math></li> <li>• <math>x, y, z \in \mathbb{F} \implies (x \oplus y) \oplus z = x \oplus (y \oplus z)</math></li> <li>• <math>\exists 0 \in \mathbb{F}</math> such that <math>\forall x \in \mathbb{F}, x \oplus 0 = x</math></li> <li>• <math>\forall x \in \mathbb{F}, \exists (-x) \in \mathbb{F}</math> such that <math>x \oplus (-x) = 0</math></li> <li>• <math>x, y \in \mathbb{F} \implies x \otimes y \in \mathbb{F}</math></li> <li>• <math>x, y \in \mathbb{F} \implies x \otimes y = y \otimes x</math></li> <li>• <math>x, y, z \in \mathbb{F} \implies (x \otimes y) \otimes z = x \otimes (y \otimes z)</math></li> <li>• <math>\exists 1 \in \mathbb{F}</math> such that <math>\forall x \in \mathbb{F}, x \otimes 1 = x</math></li> <li>• <math>\forall x \in \mathbb{F} \setminus \{0\}, \exists x^{-1} \in \mathbb{F}</math> such that <math>x \otimes x^{-1} = 1</math></li> </ul>

The first five properties correspond to the addition operation, and the last five to the multiplication operation. In order to relate both sets of properties, the following axiom is stated:

<b>Axiom</b>	Let $x, y, z \in \mathbb{F}$ . Then
Distributive law	$x \otimes (y \oplus z) = x \otimes y \oplus x \otimes z$
2.1	

<b>Theorem</b>	For any field $\mathbb{F}$ , there exists only one zero element.
Zero uniqueness	
2.1	

**Proof** Assume  $0_1$  and  $0_2$  are zeros for a field  $\mathbb{F}$ . Then

$$\forall x \in \mathbb{F} : \begin{cases} 0_1 + x = x & \text{(A)} \\ 0_2 + x = x & \text{(B)} \end{cases}$$

For both cases, let  $x$  be  $0_2$  and  $0_1$  respectively:

$$x = 0_2 \implies \text{(A)} : \quad 0_1 + 0_2 = 0_2 \quad \text{(C)}$$

$$x = 0_1 \implies \text{(B)} : \quad 0_2 + 0_1 = 0_1 \quad \text{(D)}$$

From (C) and commutativity:

$$0_2 + 0_1 = 0_2$$

Comparing this result with (D):

$$\begin{aligned} 0_2 + 0_1 = 0_2 \quad \text{and} \quad 0_2 + 0_1 = 0_1 \\ \implies 0_1 = 0_2 \end{aligned}$$

□



## 2.3 Order

**Definition**  
Ordered sets  
2.2

A set  $S$  is **ordered** when it has an ordering “ $<$ ” such that for all  $x, y \in S$ , exactly one of the following properties holds:

1.  $x = y$
2.  $x < y$
3.  $y < x$

**Definition**  
Ordered fields  
2.3

A field  $\mathbb{F}$  is **ordered** if it is also an ordered set. As a consequence, the following properties apply:

- $x, y \in \mathbb{F}, x < y \implies \forall z \in \mathbb{F}, x \oplus z < y \oplus z$
- $x, y \in \mathbb{F}, 0 < x, y \implies 0 < x \otimes y$

**Theorem**  
2.2

Given  $\mathbb{F}$  an ordered field. If  $x < y$  and  $0 < z$ , then  $x \otimes z < y \otimes z$ .

**Proof**

We prove by contradiction. Assume the opposite:

$$x \otimes z \geq y \otimes z$$

Then adding  $(-x \otimes z)$  on both sides, we maintain the ordering of the expression:

$$\begin{aligned} x \otimes z \oplus (-x \otimes z) &\geq y \otimes z \oplus (-x \otimes z) \\ 0 &\geq y \otimes z \oplus (-x \otimes z) \end{aligned}$$

Now, using Axiom 2.1, we get:

$$0 \geq z \otimes (y \oplus (-x))$$

From the initial conditions,  $x < y$  implies  $y \oplus (-x) > 0$ . Since we also have  $z > 0$ , we would expect the product of these two to be  $> 0$  by Definition 2.3 (second property). Hence:

$$0 \geq z \otimes (y \oplus (-x)) \quad \text{and} \quad 0 < z \otimes (y \oplus (-x))$$

This is a contradiction. □

From this point forward, for better readability,  $+$  and  $\cdot$  (or  $\times$ ) will be used instead of  $\oplus$  and  $\otimes$ . They will still represent the abstraction of a field’s addition and multiplication operations, without necessarily being the familiar operations we might expect them to be.

## 2.4 Completeness

**Definition** | A set  $X \subset \mathbb{F}$  ( $\mathbb{F}$  ordered field) is said to be *bounded above* (or respectively, *bounded below*) if  $\exists c \in \mathbb{F}$  such that  $\forall a \in \mathbb{F}, a \leq c$  (or respectively,  $a \geq c$ ).  $c$  is called upper (or respectively lower) bound of  $X$ .

Bounds  
2.4

**Definition** | A set that is both bounded above and below, is called *bounded*.

2.5

**Definition** | An element  $a \in X$  is called the *largest* element of  $X$  if  $\forall x \in X, x \leq a$ . Respectively,  $a \in X$  is called the *smallest* element of  $X$  if  $\forall x \in X, a \leq x$ . Simplifying the notation:

2.6

$$(a = \max X) := (a \in X \wedge \forall x \in X, x \leq a)$$

$$(a = \min X) := (a \in X \wedge \forall x \in X, a \leq x)$$

These read as *maximal* and *minimal* of  $X$ . Now, given this definition, is important to notice that not every set, not even every bounded set, has a maximal or minimal element. For example:

$$X = \{x \in \mathbb{F} \mid 0 \leq x < 1\}$$

Only has a minimal element (0), but no maximal element, since  $1 \notin X$

**Definition** | The smallest  $s \in \mathbb{F}$  that bounds  $X$  from above is called the *least upper bound* of  $X$ , and denoted  $\sup X$  (read "the supremum of  $X$ ")

Least Upper  
Bound  
2.7

$$(s = \sup X) := \forall x \in X ((x \leq s) \wedge (\forall s' < s \exists x' \in X (s' < x')))$$

Lets break this down by element

- $\forall x \in X$ : The following definition applies to the whole set  $X$ .
- $(x \leq s)$ : Given that  $s$  is an upper bound for  $X$ ...
- $(\forall s' < s) \exists x' \in X (s' < x')$ :
  - $(\forall s' < s)$ : Considering any arbitrary  $s'$  smaller than our upper bound  $s$
  - $\exists x' \in X$ : There will be an element  $x'$  in  $X$ , so that...
  - $(s' < x')$ : It is larger than the  $s'$ , making  $s'$  to **fail** to be an upper bound.

So in summary,  $s = \sup X$  if and only if,  $s$  is an upper bound, and no smaller number  $s'$  is an upper bound of  $X$ , because we can find an  $x'$  that is not bounded by it.

<b>Definition</b> Greatest Lower Bound 2.8	Similarly, the greatest $i \in X \subset \mathbb{F}$ that bounds $X$ below is called the <i>greatest lower bound</i> of $X$ , and denoted $\inf X$ (read "the infimum of $X$ ")
---	---

$$(i = \inf X) := \forall x \in X ((i \leq x) \wedge (\forall i' < i \exists x' \in X (x' < i')))$$

Thus, we have now the following definitions:

$$\begin{aligned} \sup X &:= \min\{c \in \mathbb{F} \mid \forall x \in X (x \leq c)\} \\ \inf X &:= \max\{c \in \mathbb{F} \mid \forall x \in X (c \leq x)\} \end{aligned}$$

It is important to note that the supremum and infimum of a set, as defined above, may not exist in an arbitrary ordered field  $\mathbb{F}$ . The definitions above specify what  $\sup X$  and  $\inf X$  mean *if they exist*, but they do not guarantee existence. We will address this issue shortly.

<b>Theorem</b> Uniqueness of Supremum 2.3	Let $X \subset \mathbb{F}$ be a nonempty set in an ordered field $\mathbb{F}$ . If $X$ has a supremum, then this supremum is unique.
--	--

<b>Proof</b>	<p>Suppose <math>s_1</math> and <math>s_2</math> are both suprema of <math>X</math>. We will show that <math>s_1 = s_2</math>. Since <math>s_1 = \sup X</math>, we know that <math>s_1</math> is an upper bound of <math>X</math>. Since <math>s_2 = \sup X</math>, we know that <math>s_2</math> is the <i>least</i> upper bound of <math>X</math>. Therefore:</p> $s_2 \leq s_1$ <p>By the same reasoning (swapping the roles of <math>s_1</math> and <math>s_2</math>), since <math>s_2</math> is an upper bound and <math>s_1</math> is the least upper bound:</p> $s_1 \leq s_2$ <p>By the antisymmetry property of order in <math>\mathbb{F}</math>, we have <math>s_1 \leq s_2</math> and <math>s_2 \leq s_1</math>, which implies:</p> $s_1 = s_2$ <p>Therefore, the supremum is unique. <span style="float: right;">□</span></p>
--------------	---

The proof for the uniqueness of the infimum is analogous.

**Example**

2.1

Consider the ordered field  $\mathbb{Q}$  of rational numbers, and let:

$$S = \{x \in \mathbb{Q} \mid x^2 < 2\}$$

The set  $S$  is nonempty (for instance,  $1 \in S$ ) and bounded above (for instance,  $2 \in \mathbb{F}$  is an upper bound). However,  $S$  does not have a supremum in  $\mathbb{Q}$ , since if it had, it would have to equal  $\sqrt{2} \notin \mathbb{Q}$ , so  $S$  has no least upper bound within the rational numbers.

This shows that not every ordered field has the property that bounded sets possess suprema.

**Definition**

Complete Ordered

Field

2.9

An ordered field  $\mathbb{F}$  is called *complete* if every nonempty subset of  $\mathbb{F}$  that is bounded above has a supremum in  $\mathbb{F}$ .

**Proposition**

2.1

If  $\mathbb{F}$  is a complete ordered field, then every nonempty subset of  $\mathbb{F}$  that is bounded below has an infimum in  $\mathbb{F}$ .

**Proof** Let  $X \subset \mathbb{F}$  be nonempty and bounded below. Define:

$$X' = \{-x \mid x \in X\}$$

**1.  $X'$  is nonempty and bounded above**

Since  $X$  is nonempty,  $\exists x_0 \in X \Rightarrow -x_0 \in X'$  by definition of  $X'$ . Thus  $X' \neq \emptyset$ .  
Now,  $X$  is bounded below by the proposition, so there exists  $c \in \mathbb{F}$  such that:

$$\begin{aligned} \forall x \in X, \quad c &\leq x \\ \forall x \in X, \quad -x &\leq -c \end{aligned}$$

Since  $-x \in X'$  and  $-c \in \mathbb{F}$ , we can be sure that  $X'$  is bounded above in  $\mathbb{F}$ .  
Considering  $\mathbb{F}$  is complete, and we proved  $X'$  is nonempty and bounded above,  $X'$  has a supremum in  $\mathbb{F}$ .

**2.  $-s$  is a lower bound for  $X$ .**

Let  $s = \sup X'$  and  $x \in X$  be arbitrary. Then  $-x \in X'$  by definition of  $X'$ . Since  $s$  is an upper bound for  $X'$ :

$$\begin{aligned} \forall -x \in X', \quad -x &\leq s \\ \Rightarrow \quad -s &\leq x \end{aligned}$$

Showing that  $-s$  is a lower bound for  $X$ .

**3:  $-s$  is the greatest lower bound for  $X$ .**

Let  $\ell \in \mathbb{F}$  be any lower bound for  $X$ .

Since  $\ell$  is a lower bound for  $X$ :

$$\begin{aligned} \forall x \in X, \quad \ell &\leq x \\ \Rightarrow \quad -x &\leq -\ell \end{aligned}$$

Meaning that  $-\ell$  is an upper bound for any  $-x \in X'$ . Since  $s = \sup X'$ , we have:

$$\begin{aligned} s &\leq -\ell \\ \Rightarrow \ell &\leq -s \end{aligned}$$

Showing that  $-s$  is greater than or equal to every lower bound of  $X$ . Therefore,  $-s = \inf X$ .  $\square$

**Theorem**  
Least Upper  
Bound Principle  
2.4

Let  $\mathbb{F}$  be a complete ordered field. Every nonempty subset of  $\mathbb{F}$  that is bounded above has a unique least upper bound in  $\mathbb{F}$ .

**Proof**

Let  $X \subset \mathbb{F}$  be nonempty and bounded above.

**Existence:** Since  $\mathbb{F}$  is complete, by definition of completeness,  $X$  has a supremum in  $\mathbb{F}$ .

**Uniqueness:** By the Uniqueness of Supremum theorem, this supremum is unique. Therefore,  $X$  has a unique least upper bound.  $\square$

## 2.5 Archimedean property

Now that we achieved completeness on an ordered field, we can now extend the definitions and properties into a theorem/property that uses the result from the *Least Upper Bound principle* (Theorem 2.4).

**Theorem**  
2.5

Let  $\mathbb{F}$  be a complete ordered field, then

$$\forall x \in \mathbb{F}, \exists! n \in \mathbb{N} \subset \mathbb{F} : n > x$$

**Proof** We first define the subset  $\mathbb{N} \subset \mathbb{F}$  **inductively**, to work with a generalized version of the set of “natural numbers”

1.  $1_{\mathbb{F}}$  is the multiplicative identity in  $\mathbb{F}$
2.  $n + 1_{\mathbb{F}} \in \mathbb{N}, \forall n \in \mathbb{N}$  defines the induction step over  $\mathbb{N}$ , using the addition operation from the field  $\mathbb{F}$

We now proceed to prove by contradiction, assuming  $\exists x \in \mathbb{F}, \forall n \in \mathbb{N} :$

$$n \leq x$$

Meaning that  $\mathbb{N}$  is bounded above. Now, since  $\mathbb{N}$  is not empty, and is bounded by an element of the (complete ordered) field that contains it ( $x \in \mathbb{F}$ ), then by *L.U.B. principle* (Theorem 2.4),  $\mathbb{N}$  must have a supremum.

Let  $s := \sup \mathbb{N} \in \mathbb{F}$  be that supremum of  $\mathbb{N}$ . Then, since  $s$  is the least upper bound, any element that is less than  $s$  will no longer be an upper bound for  $\mathbb{N}$ . Conveniently we take  $s - 1_{\mathbb{F}}$ :

$$\begin{aligned} \exists n_0 \in \mathbb{N} : s - 1_{\mathbb{F}} &< n_0 \\ \Rightarrow s &< n_0 + 1_{\mathbb{F}} \end{aligned}$$

But by our inductive definition of  $\mathbb{N} : (n_0 + 1_{\mathbb{F}}) \in \mathbb{N}$ . So we found out that  $s$  ( $\sup \mathbb{N}$ ) fails to be an upper bound for an element in  $\mathbb{N}$ .

Therefore, our original assumption of  $x$  must be wrong. □

Now, is important to notice that  $\mathbb{F}$  implies an archimedien field, but the opposite won't necessarily be true.

**Example**  
2.2

Using an Archimedean field, that is not complete, lets take  $\mathbb{F} = \mathbb{Q}$

$$x \in \mathbb{Q} \wedge n \in \mathbb{N} \subset \mathbb{Q}$$

It is true that, for any  $x$  there is a natural number  $n$  so that

$$n > x$$

But invoking the previous example (Example 2.1) we can take a subset of  $\mathbb{Q}$  that is not bounded in  $\mathbb{Q}$ , failing to properly form a complete set.

Closing this chapter, lets emphasise the fact that the construction of  $\mathbb{N} \subset \mathbb{F}$  by induction was crucial to generalize the property for any complete ordered field. Next we will explain why this wasn't necessary at all.



### 3 $\mathbb{R}$ as the complete ordered field

#### 3.1 $\mathbb{F}$ is $\mathbb{R}$

Turns out that there is a reason why it is called **Real** Analysis. So far we have worked over a generic *Complete Ordered Field*  $\mathbb{F}$ , that was also an *Archimedean* following the expected properties. We have finally reached the point where we can state that **any** set that manages to follow all these properties is actually identical to the set of real numbers  $\mathbb{R}$ . In fact,  $\mathbb{R}$  is the only set that accomplishes this.

Most Real Analysis courses don't go into proving this, but as I already mentioned in the first chapter, I want to cover all doubts and missing points existent during a course like this.

We will go through the initial proofs needed to understand the main one. At the beginning it's possible that some of them look unnecessary or trivial, but I don't want to assume that much. Better to be safe than sorry.

##### 3.1.1 Isomorphism

Our starting point will be defining what it means to have "equal fields".

<b>Definition</b>	Let $F, F'$ fields. A function $\phi : F \rightarrow F'$ is a homomorphism between $F$ and $F'$ iff. it preserves the defined operations in both fields:
Field homomorphism	
3.1	$\phi(x + y) = \phi(x) + \phi(y), \forall x, y \in F$ $\phi(x \cdot y) = \phi(x) \cdot \phi(y), \forall x, y \in F$

<b>Definition</b>	Let $F, F'$ fields. A function $\phi : F \rightarrow F'$ is a isomorphism iff. it is a homomorphism and also a bijection
Field isomorphism	
3.2	

**Lemma** | Let  $F, F'$  fields,  $\phi : F \rightarrow F'$ . If  $\phi$  preserves order from  $\mathbb{F}$ :  
 Injectivity by  
 order preservation  
 3.1 | Then  $\phi$  is injective.

$$x < y \Rightarrow \phi(x) < \phi(y), x, y \in F$$

**Proof** | To prove injectivity, we need to show that for any two identical images of the function  $\phi$ , we get that their arguments were the same, guaranteeing the uniqueness of the image:  
 Let  $x, y \in \mathbb{F}$  so that  

$$\phi(x) = \phi(y)$$
  
 Using the tricotomy over  $F$ :  
 Case 1:  $x < y$ :  

$$\rightarrow \phi(x) < \phi(y) (\rightarrow \leftarrow)$$
  
 Case 2:  $y < x$ :  

$$\rightarrow \phi(y) < \phi(x) (\rightarrow \leftarrow)$$
  

$$\Rightarrow x = y$$
  
 Then,  $\phi$  is injective. □

**Lemma** | Let  $F, F'$  fields,  $\phi : F \rightarrow F'$ . Define:  
 Surjectivity by  
 construction  
 3.2 | Then, the bounded function  $\phi' : F \rightarrow \text{Im}_F$  is surjective

$$\text{Im}_F := \{\phi(x), x \in F\}$$

**Proof** To prove surjectivity, we need to show that every element in  $y \in \text{Im}_F$  has a  $x \in F$  such that  $\phi'(x) = y$   
 Using the definition of our constructed set:

$$\begin{aligned} \forall y \in \text{Im}_F &\Leftrightarrow y \in \{\phi(x), x \in F\} \\ \Rightarrow \exists x \in F / \forall y \in \text{Im}_F : y &= \phi'(x) \end{aligned}$$

Finally proving that for any image of  $\phi' \in \text{Im}_F$  we will have a preimage  $x \in F$ .  
 Then  $\phi'$  is surjective.  $\square$

On this first part, this surjectiveness by construction might be the bit that doesn't quite seem correct. Isn't it trivial to have surjectiveness if we grab the method  $\phi$  and limit it to its image  $\phi'$ ?

The key here is that we defined the set of images  $\text{Im}_F$  first, and *then* proved the surjectiveness in it. The lemma confirms that the set we defined was *just right*. Not so big to leave some elements unreached, and not too small to make undefined preimages at some spots.

### 3.1.2 Sets construction