Section 1.1: Definition and Properties of Real Numbers

We will give an axiomatic definition of the real numbers. We will define the *set of real numbers*:

- Denoted by $\mathbb{R}$,
- As a set with two operations $+$ (addition) and $\cdot$ (multiplication),
- As well as an ordering $<$,
- Which satisfy
  - The laws of addition (A),
  - The laws of multiplication (M),
  - The distributive law (D),
  - The order laws (O) and
  - The Dedekind Completeness Axiom (C).

These laws and axioms will be given and discussed below.

Remember: An *axiom* is a true mathematical statement whose truth is accepted without a proof.

Addition and multiplication are maps which assign to every two elements in $a, b \in \mathbb{R}$ an element in $\mathbb{R}$ which is denoted by $a + b$ and $a \cdot b$ (in general, written ab), respectively. We require that these operations satisfy the following axioms.

Preliminary properties:

- The *transitive property* of equality:

$$\text{If } a = b \text{ and } b = c, \text{ then } a = c.$$

- The *closure properties* of addition and multiplication:

For all real numbers a and b, there are unique real numbers $a + b$ and ab.

A. Axioms of addition

(A1) Associative Law: $a + (b + c) = (a + b) + c$ for all $a, b, c \in \mathbb{R}$.

(A2) Commutative Law: $a + b = b + a$ for all $a, b \in \mathbb{R}$.

(A3) Zero: There is a real number 0 such that $a + 0 = a$ for all $a \in \mathbb{R}$.

(A4) Additive inverse: For each $a \in \mathbb{R}$ there is $-a \in \mathbb{R}$ such that $a + (-a) = 0$.

Notation

For $a, b \in \mathbb{R}$ one writes $a - b := a + (-b)$. (Definition of *subtraction*)

Additional Notes

1. Any set with the operation $+$ satisfying (A1), (A3) and (A4) is called a *group*. If also (A2) is satisfied, the group is called an *Abelian* (or commutative) *group*.
2. You will encounter detailed discussions of (Abelian) groups in algebra courses.
3. The additive inverse of a number is also called the *negation* of a number.

Theorem 1.1 (Basic group properties)

(a) *The number* 0 *is unique.*
(b) *For all* $a \in \mathbb{R}$*, the number* $-a$ *is unique.*
(c) *For all* $a, b \in \mathbb{R}$*, the equation* $a + x = b$ *has a unique solution. This solution is* $x = b - a$.
(d) $\forall a \in \mathbb{R}; -(-a) = a$.
(e) $\forall a, b \in \mathbb{R}; -(a + b) = -a - b$.
(f) $-0 = 0$.

*Note that (b) allows us to say that if $a + b = 0$, then $b = -a$.

Proof (We can only use the axioms of addition at this stage!)

(a) *The number* 0 *is unique.*

Let $0, 0' \in \mathbb{R}$ such that $a + 0 = a$ and $a + 0' = a$ for all $a \in \mathbb{R}$. We must show that $0 = 0'$:

0	$= 0 + 0'$	assumption with $a = 0$.
	$= 0' + 0$	(A2)
	$= 0'$	assumption with $a = 0'$.

(b) *For all* $a \in \mathbb{R}$*, the number* $-a$ *is unique.*

Let $a \in \mathbb{R}$ and $a', a'' \in \mathbb{R}$ such that $a + a' = 0$ and $a + a'' = 0$. We must show that $a' = a''$:

a'	$= a' + 0$	(A3)
	$= a' + (a + a'')$	assumption
	$= (a' + a) + a''$	(A1)
	$= (a + a') + a''$	(A2)
	$= 0 + a''$	assumption
	$= a'' + 0$	(A2)
	$= a''$	(A3)

(c) *For all $a, b \in \mathbb{R}$, the equation $a + x = b$ has a unique solution. This solution is $x = b - a$.*

First we show that $x = b - a$ is a solution. So let $x = b - a$. Then

$$
\begin{aligned}
a + x &= a + (b - a) && \text{substitution} \\
&= a + \big(b + (-a)\big) && \text{definition of subtraction} \\
&= a + ((-a) + b) && \text{(A2)} \\
&= \big(a + (-a)\big) + b && \text{(A1)} \\
&= 0 + b && \text{(A4)} \\
&= b + 0 && \text{(A2)} \\
&= b && \text{(A3)}
\end{aligned}
$$

To show that the solution is unique let $x \in \mathbb{R}$ such that $a + x = b$. Then

$$
\begin{aligned}
x &= x + 0 && \text{(A3)} \\
&= x + \big(a + (-a)\big) && \text{(A4)} \\
&= (x + a) + (-a) && \text{(A1)} \\
&= (a + x) + (-a) && \text{(A2)} \\
&= b - a && \therefore a + x = b
\end{aligned}
$$

This shows that the solution is unique.

(d) $\forall a \in \mathbb{R}; -(-a) = a.$

Note that

$$(-a) + \big(-(-a)\big) = 0. \qquad \text{(A4)}$$

On the other hand,

$$
\begin{aligned}
(-a) + a &= a + (-a) && \text{(A2)} \\
&= 0. && \text{(A4)}
\end{aligned}
$$

By part (b), it follows that $-(-a) = a$.

Alternatively:

$$\begin{aligned}
-(-a) &= -(-a) + 0 && \text{(A3)} \\
&= -(-a) + \big(a + (-a)\big) && \text{(A4)} \\
&= \big(a + (-a)\big) + \big(-(-a)\big) && \text{(A2)} \\
&= a + \Big((-a) + \big(-(-a)\big)\Big) && \text{(A1)} \\
&= a + 0 && \text{(A4)} \\
&= a && \text{(A3)}
\end{aligned}$$

(e) $\forall a, b \in \mathbb{R}; -(a + b) = -a - b$.

$$\begin{aligned}
(a + b) + (-a - b) &= (a + b) + \big((-a) + (-b)\big) && \text{definition of subtraction} \\
&= (b + a) + \big((-a) + (-b)\big) && \text{(A2)} \\
&= \big((b + a) + (-a)\big) + (-b) && \text{(A1)} \\
&= \Big(b + \big(a + (-a)\big)\Big) + (-b) && \text{(A1)} \\
&= (b + 0) + (-b) && \text{(A4)} \\
&= b + (-b) && \text{(A3)} \\
&= 0 && \text{(A4)}
\end{aligned}$$

By part (b), $-(a + b) = -a - b$.

(f) $-0 = 0$.

Since

$$0 + 0 = 0 \qquad \text{(A3)}$$

and

$$0 + (-0) = 0 \qquad \text{(A4)}$$

we have

$$-0 = 0 \qquad \text{Part (b).}$$

■

M. Axioms of multiplication

(M1) Associative Law: $a(bc) = (ab)c$ for all $a, b, c \in \mathbb{R}$.

(M2) Commutative Law: $ab = ba$ for all $a, b \in \mathbb{R}$.

(M3) One: There is a real number 1 such that $1 \neq 0$ and $a \cdot 1 = a$ for all $a \in \mathbb{R}$.

(M4) Multiplicative inverse: For each $a \in \mathbb{R}$ with $a \neq 0$ there is $a^{-1} \in \mathbb{R}$ such that $aa^{-1} = 1$.

Notation

For $a, b \in \mathbb{R}$ one writes $\frac{a}{b} = a \div b := b^{-1}a$ where $b^{-1} = \frac{1}{b}$. (Definition of *division*)

D. The distributive law axiom

(D) Distributive Law: $a(b + c) = ab + ac$ for all $a, b, c \in \mathbb{R}$.

Additional Notes

1. Any set with the operations $+$, $\cdot$ satisfying the axioms (A1)–(A4), (M1)–(M4) and (D) is called a *field*.
2. You will encounter detailed discussions of fields in algebra courses.
3. The multiplicative inverse of a number is also briefly called the *inverse* of a number.
4. The set of nonzero real numbers, $\mathbb{R}\backslash\{0\}$, is an Abelian group with respect to multiplication.

Theorem 1.2 (Basic field properties: Distributive laws)

(a) $\forall a, b, c \in \mathbb{R}, (a + b)c = ac + bc.$
(b) $\forall a \in \mathbb{R}, a \cdot 0 = 0.$
(c) $\forall a, b \in \mathbb{R}, ab = 0 \Leftrightarrow a = 0 \text{ or } b = 0.$
(d) $\forall a, b \in \mathbb{R}, (-a)b = -(ab).$
(e) $\forall a \in \mathbb{R}, (-1)a = -a.$
(f) $\forall a, b \in \mathbb{R}, (-a)(-b) = ab.$

Proof

(a) $\forall a, b, c \in \mathbb{R}, (a + b)c = ac + bc.$

$$\begin{aligned}(a+b)c &= c(a+b) && \text{(M2)}\\ &= ca + cb && \text{(D)}\\ &= ac + bc. && \text{(M2)}\end{aligned}$$

(b) $\forall a \in \mathbb{R},\ a \cdot 0 = 0.$

Since

$$\begin{aligned} a \cdot 0 &= a(0+0) && \text{(A3)} \\ &= a \cdot 0 + a \cdot 0 && \text{(D)} \end{aligned}$$

and

$$\begin{aligned} a \cdot 0 &= a \cdot 0 + 0 && \text{(A3)} \\ &= 0 + a \cdot 0 && \text{(A2)} \end{aligned}$$

by Theorem 1.1(c) we have $a \cdot 0 = 0$.

(c) $\forall a, b \in \mathbb{R},\ ab = 0 \Leftrightarrow a = 0 \text{ or } b = 0.$

($\Leftarrow$) $a = 0$ or $b = 0$:

- If $b = 0$, then

$$\begin{aligned} ab &= a \cdot 0 && \text{substitution} \\ &= 0 && \text{Part (b).} \end{aligned}$$

- If $a = 0$, then

$$\begin{aligned} ab &= ba && \text{(M2)} \\ &= b \cdot 0 && \text{substitution} \\ &= 0 && \text{Part (b).} \end{aligned}$$

($\Rightarrow$) Now assume that $ab = 0$.

- If $b = 0$, the property "$a = 0$ or $b = 0$" follows.

- So now assume $b \neq 0$. Then

$$\begin{aligned} a &= a \cdot 1 && \text{(M3)} \\ &= a(bb^{-1}) && \text{(M4)} \\ &= (ab)b^{-1} && \text{(M1)} \\ &= 0 \cdot b^{-1} && \text{assumption} \\ &= b^{-1} \cdot 0 && \text{(M2)} \\ &= 0 && \text{Part (b).} \end{aligned}$$

(d) $\forall a, b \in \mathbb{R}$, $(-a)b = -(ab)$.

Using field laws, we get

$$\begin{aligned} ab + (-a)b &= \big(a + (-a)\big)b && \text{Part (a)} \\ &= 0 \cdot b && \text{A4} \\ &= b \cdot 0 && \text{M2} \\ &= 0 && \text{Part (b)} \end{aligned}$$

and from Theorem 1.1(b),

$$(-a)b = -ab.$$

(e) $\forall a \in \mathbb{R}$, $(-1)a = -a$.

Is a special case of Part (d). Let $b = 1$. Then

$$\begin{aligned} -a &= -(a \cdot 1) && \text{M3} \\ &= -(1 \cdot a) && \text{M2} \\ &= (-1)a && \text{Part (d).} \end{aligned}$$

(f) $\forall a, b \in \mathbb{R}$, $(-a)(-b) = ab$.

From (d) and other laws and rules we find

$$\begin{aligned} (-a)(-b) &= -[a(-b)] && \text{Part (d)} \\ &= -[(-b)a] && \text{M2} \\ &= -[-ba] && \text{Part (d)} \\ &= ba && \text{Theorem 1.1 (d)} \\ &= ab && \text{M2.} \end{aligned}$$

■

Theorem 1.3 (Basic field properties: multiplication)

(a) *The number* 1 *is unique.*
(b) *For all* $a \in \mathbb{R}$ *with* $a \neq 0$, *the number* a^{-1} *is unique.*
(c) *For all* $a, b \in \mathbb{R}$ *with* $a \neq 0$, *the equation* $ax = b$ *has a unique solution. This solution is*
$x = a^{-1}b$.
(d) $\forall a \in \mathbb{R}\backslash\{0\}$, $(a^{-1})^{-1} = a$.
(e) $\forall a, b \in \mathbb{R}\backslash\{0\}$, $(ab)^{-1} = a^{-1}b^{-1}$.
(f) $\forall a \in \mathbb{R}\backslash\{0\}$, $(-a)^{-1} = -a^{-1}$.
(g) $1^{-1} = 1$.

Proof

See tutorials. The proofs are similar to those of Theorem 1.1. ■

Next we give the axioms for the set of positive real numbers. It is convenient to use the notation $a > 0$ for *positive numbers* a.

O. The order axioms

(O1) Trichotomy: For each $a \in \mathbb{R}$, exactly one of the following statements is true:

$$a > 0 \text{ or } a = 0 \text{ or } -a > 0.$$

(O2) If $a > 0$ and $b > 0$, then $a + b > 0$.

(O3) If $a > 0$ and $b > 0$, then $ab > 0$.

The definition of positivity of real numbers gives rise to an order relation for real numbers:

Definition Let $a, b \in \mathbb{R}$. Then a is called *larger than* b, written $a > b$, if $a - b > 0$.

Notes

1. Since $a - 0 = a$, the notation $a > 0$ is consistent.
2. It is convenient to introduce the following notations:
   - $a \geq b \Leftrightarrow a > b$ or $a = b$
   - $a < b \Leftrightarrow b > a$
   - $a \leq b \Leftrightarrow a < b$ or $a = b$
3. We will define general powers later. Below we use the notation $a^2 = a \cdot a$.

Theorem 1.4 (Basic order properties)

Let $a, b, c, d \in \mathbb{R}$. Then

(a) $a < 0 \Leftrightarrow -a > 0$.
(b) $a < b$ *and* $b < c \Rightarrow a < c$.
(c) $a < b \Rightarrow a + c < b + c$.
(d) $a < b$ *and* $c < d \Rightarrow a + c < b + d$.
(e) $a < b$ *and* $c > 0 \Rightarrow ca < cb$.
(f) $0 \leq a < b$ *and* $0 \leq c < d \Rightarrow ac < bd$.
(g) $a < b$ *and* $c < 0 \Rightarrow ca > cb$.
(h) $a \neq 0 \Rightarrow a^2 > 0$.
(i) $a > 0 \Rightarrow a^{-1} > 0$ *and* $a < 0 \Rightarrow a^{-1} < 0$.
(j) $0 < a < b \Rightarrow b^{-1} < a^{-1}$.
(k) $1 > 0$.

Proof

(a), (b), (h), (i), (j), (k) in class. For (c) - (g) see tutorials.

(a) $a < 0 \Leftrightarrow -a > 0$.

$$\begin{aligned} a < 0 &\Leftrightarrow 0 > a && \text{by definition of } < \\ &\Leftrightarrow 0 - a > 0 && \text{by definition of } > \\ &\Leftrightarrow -a > 0 && \text{since } 0 - a = -a + 0 = -a \text{ (add reasons)} \end{aligned}$$

(b) $a < b$ *and* $b < c \Rightarrow a < c$.

$$\begin{aligned} a < b \text{ and } b < c \quad &\Rightarrow b - a > 0 \text{ and } c - b > 0 && \text{by definition} \\ &\Rightarrow (b - a) + (c - b) > 0 && \text{by (O2)} \\ &\Rightarrow c - a > 0 && \text{by (A1)-(A4)} \\ &\Rightarrow a < c && \text{by definition} \end{aligned}$$

(h) $a \neq 0 \Rightarrow a^2 > 0$.

Since $a \neq 0$, either $a > 0$ or $a < 0$.

- If $a > 0$, then $a^2 = aa > 0$ by (O3).
- If $a < 0$, then $-a > 0$ by part (a) and $a^2 = (-a)(-a)$ by Theorem 1.2, (f). Hence $a^2 = (-a)(-a) > 0$ by (O3).

(i) $a > 0 \Rightarrow a^{-1} > 0$ *and* $a < 0 \Rightarrow a^{-1} < 0$.

Since $a \neq 0$, a^{-1} exists with $aa^{-1} = 1$ by (M4). Then $a^{-1} \neq 0$ by Theorem 1.2, (c). Hence $(a^{-1})^2 > 0$ by (h). Thus, if $a > 0$, $a^{-1} = a(a^{-1})^2 > 0$ by (O3).

Similarly, use (g) if $a < 0$. (Add these steps.)

(j) $0 < a < b \Rightarrow b^{-1} < a^{-1}$.

By (i), $a^{-1} > 0$ and $b^{-1} > 0$. Hence $a^{-1}b^{-1} > 0$ by (O3). Then

$$\begin{aligned} b^{-1} &= a(a^{-1}b^{-1}) && \text{by (M1) - (M4)} \\ &< b(a^{-1}b^{-1}) && \text{by Part (e)} \\ &= (bb^{-1})a^{-1} && \text{by (M1) and (M2)} \\ &= a^{-1} && \text{by (M3) and (M4)} \end{aligned}$$

(k) $1 > 0$.

$$\begin{aligned} 1 &= 1 \cdot 1 && \text{by (M3)} \\ &= 1^2 && \text{by definition} \\ &> 0 && \text{by Part (h).} \end{aligned}$$

■

There is still one axiom missing, the axiom of Dedekind Completeness. However, we will postpone the formulation of this axiom to the next section since we need some further definitions.

* * * * * * *