1. Algebraic Properties of the Real Numbers

1.1 Axioms (Algebraic Axioms for the Real Numbers ("Field Axioms")). We assume that the real numbers consists of a set $\mathbb{R}$ equipped with two binary operations " $+$ " and " $\cdot$ " satisfying the following axioms:

AC (Commutativity of Addition)

$$a + b = b + a \text{ for all } a, b \in \mathbb{R}.$$

AA (Associativity of Addition)

$$a + (b + c) = (a + b) + c \text{ for all } a, b, c \in \mathbb{R}.$$

AID (Existence of Additive Identity) There is a number $0 \in \mathbb{R}$ satisfying

$$a + 0 = a = 0 + a \text{ for all } a \in \mathbb{R}.$$

AIV (Existence of Additive Inverses) Corresponding to each $a \in \mathbb{R}$, there is a unique number $-a \in \mathbb{R}$ satisfying

$$a + (-a) = 0 = (-a) + a.$$

MC (Commutativity of Multiplication)

$$ab = ba \text{ for all } a, b \in \mathbb{R}.$$

MA (Associativity of Multiplication)

$$a(bc) = (ab)c \text{ for all } a, b, c \in \mathbb{R}.$$

MID (Existence of Multiplicative Identity) There is a number 1 (different from 0) in $\mathbb{R}$ satisfying

$$1a = a = a1 \text{ for all } a \in \mathbb{R}.$$

MIV (Existence of Multiplicative Inverses) Corresponding to each a (except 0) in $\mathbb{R}$, there is a unique number $a^{-1} \in \mathbb{R}$ satisfying

$$aa^{-1} = 1 = a^{-1}a.$$

D (Distributivity)

$$a(b + c) = ab + ac \text{ and } (a + b)c = ac + bc \text{ for all } a, b, c \in \mathbb{R}.$$

1.2 Remark. Some other basic facts will be used in proofs without being formally stated here and without citation (except as needed to clarify the exposition). These can be divided into two categories:

1. **Laws of logic.**
2. **Laws of equality.** First, we have three basic axioms: For all a, b and c we have (i) $a = a$, (ii) if $a = b$ then $b = c$, and (iii) if $a = b$ and $b = c$ then $a = c$. In addition there is a general principle which we may call *substitution of equals*, stating that if $a = b$ then we may freely substitute the symbol b for a in any expression. Thus, if $a = b$ and $c = d$ then $a + c = b + d$ and $ac = bd$. The principle here is that $a = b$ means that the symbols a and b are *names for the same object*. All of the properties with which we are concerned are properties of the underlying object, not of the name, and hence are unaffected by which name we happen to use for the object.

1.3 Definition/Remark. A *binary operation* on a set S is a function that assigns to every ordered pair of elements of S a unique element of S. Familiar examples of binary operations on $\mathbb{R}$ are ordinary addition, subtraction, and multiplication. In particular, if we write $a+b = c$, we are assigning the real number c (the "answer") to the ordered pair (a, b) of real numbers.

One immediate consequence of this definition is the familiar "equals added to equals are equal". In other words, if $a = b$ and $c = d$, then $a + c = b + d$. The justification for this is that our binary operation of addition assigns to the ordered pair (a, c) some real number e, let's say. But since $a = b$ and $c = d$, the ordered pair (b, d) is the *same* ordered pair as (a, c), and since the operation of addition assigns a *unique* number e to this ordered pair, we must have $b + d = e$. But since $a + c = e$ we have $a + c = b + d$. In summary, we can say that the definition of binary operation justifies the implication that if $a = b$ and $c = d$, then $a + c = b + d$. Similar considerations apply to subtraction, multiplication, and division.

We will use the familiar rule that multiplication takes precidence over addition, so that $ab + cd$ means $(ab) + (cd)$.

1.4 Theorem. *Suppose $a, b, c, d \in \mathbb{R}$. Then*

a). *If $a + c = b + c$, then $a = b$.*

b). *The additive identity is unique.*
That is, if $e \in \mathbb{R}$ and $a + e = a = e + a$ for all $a \in \mathbb{R}$, then $e = 0$.

c). *If $ac = bc$ and $c \neq 0$, then $a = b$.*

d). *The multiplicative identity is unique.*
That is, if $e \in \mathbb{R}$ and $a \cdot e = a = e \cdot a$ for all $a \in \mathbb{R}$, then $e = 1$.

e). $(a + b) + (c + d) = (a + c) + (b + d)$ *and* $(ab)(cd) = (ac)(bd)$.

f). $a0 = 0 = 0a$.

g). *If $ab = 0$, then $a = 0$ or $b = 0$.*

h). $(-1)a = -a$.

i). $-(-a) = a$ *and* $-(a + b) = (-a) + (-b)$.
Warning: You cannot use the identity "$(-1)(-1) = 1$" in the proof of clause (i), since you will not have proved it until clause (j).

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

k). If $a \neq 0$, then $a^{-1} \neq 0$.

l). If $a \neq 0$, then $(a^{-1})^{-1} = a$; also if $a \neq 0$ and $b \neq 0$, then $(ab)^{-1} = a^{-1}b^{-1}$.

1.5 Theorem. *Suppose $a, b \in R$.*

a). The equation $b + x = a$ has one and only one solution.

b). If $b \neq 0$, then the equation $bx = a$ has one and only one solution.

1.6 Definition. We define subtraction and division as follows.

a). For $a, b \in \mathbb{R}$, $a - b$ denotes that number x such that $b + x = a$.

b). For $a, b \in \mathbb{R}$ with $b \neq 0$, $\frac{a}{b}$ denotes that number x such that $bx = a$.

1.7 Theorem. *Suppose $a, b, c, d \in R$.*

a). $a - b = a + (-b)$; also, if $b \neq 0$, then $\frac{a}{b} = ab^{-1}$.

b). $a(b - c) = ab - ac$ and $-(a - b) = b - a$.

c). If $a \neq 0$, then $\frac{1}{a}$ is the multiplicative inverse of a.

d). $\frac{a}{1} = a$; also, if $a \neq 0$, then $\frac{a}{a} = 1$.

e). If $b \neq 0$, then $\frac{-a}{b} = \frac{a}{-b} = -\left(\frac{a}{b}\right)$ and $\frac{-a}{-b} = \frac{a}{b}$.

f). If $b \neq 0$ and $d \neq 0$, then $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$.

g). If $b \neq 0$, $c \neq 0$ and $d \neq 0$, then $\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$.

h). If $b \neq 0$ and $d \neq 0$, then $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$.

1.13 Axioms (Order Axioms for the Real Numbers). We assume that there is a binary relation " $<$ " on $\mathbb{R}$ satisfying the following axioms:

OTC (Trichotomy)
For any $a, b \in R$, exactly one of $a < b$, $a = b$, and $b < a$ holds.

OTR (Transitivity)
If $a < b$ and $b < c$, then $a < c$.

OA (Compatibility with Addition)
If $a < b$, then $a + c < b + c$.

OM (Compatibility with Multiplication)
If $a < b$ and $0 < c$, then $ac < bc$.

LUB (Least Upper Bound) This axiom will be presented in Chapter 4.

1.14 Notation. "$a > b$" means "$b < a$", "$a \leq b$" means "$a < b$ or $a = b$", etc.

1.15 Theorem. *Suppose $a, b, c \in \mathbb{R}$. Then*

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

b). If $a < b$, then $-a > -b$.

c). If $a < b$ and $c < 0$, then $ac > bc$.

d). $a > 0, b > 0$ imply $ab > 0$; $a > 0, b < 0$ imply $ab < 0$; and $a < 0, b < 0$ imply $ab > 0$.

e). $ab > 0$ implies that either $a > 0$ and $b > 0$ or else $a < 0$ and $b < 0$.

f). $0 < 1$.

g). $a - 1 < a < a + 1$.

h). Suppose $a \neq 0$. Then $a > 0$ iff $\frac{1}{a} > 0$.

i). Suppose $b \neq 0$. Then $\frac{a}{b} > 0$ iff either $a > 0$ and $b > 0$ or $a < 0$ and $b < 0$.

j). Suppose a and b are either both positive or both negative. Then $a < b$ iff $\frac{1}{a} > \frac{1}{b}$.

k). If $a^2 < b^2$ and $a, b \geq 0$, then $a < b$.

1.16 Exercise. Prove or disprove each of the following.

a). If $a < b$ and $c < d$, then $a + c < b + d$.

b). If $a < b$ and $c < d$, then $ac < bd$.

c). Formulate true versions of the statements you disproved.