

EQUALITY

Equality is the most fundamental relation in all of mathematics. It can be used between any two mathematical objects of the same type, such as numbers, matrices, ordered pairs, sets, functions, etc. To say that $a = b$ is simply to say that the symbols a and b represent the very same object. Equality always has the following fundamental properties.

- (REFLEXIVITY) $a = a$.
- (SYMMETRY) If $a = b$, then $b = a$.
- (TRANSITIVITY) If $a = b$ and $b = c$, then $a = c$.
- (SUBSTITUTION) If $a = b$, then b may be substituted for any or all occurrences of a in any mathematical statement without affecting that statement's truth value.

Most of the familiar rules for “doing the same thing to both sides of an equation” are really just applications of these properties. For example, suppose $a = b$ and c is any number at all. The reflexive property shows that $a + c = a + c$, and then substituting b for a on the right-hand side (but not the left) leads to $a + c = b + c$.

PRIMITIVE TERMS

To avoid circularity, we cannot give every term a rigorous mathematical definition; we have to accept some things as undefined terms. For this course, we will take the following fundamental notions as primitive undefined terms. You already know intuitively what these terms mean; but the only facts about them that can be used in proofs are the ones expressed in the axioms listed below (and any theorems that can be proved from the axioms).

- *Real number*
- *Addition*
- *Multiplication*
- *Positive*

These terms are assumed to satisfy certain axioms. The axioms come in three groups.

GROUP I: FIELD AXIOMS

We assume that there exists a set \mathbb{R} , whose elements are called *real numbers*, endowed with two binary operations called *addition* (denoted by $a + b$) and *multiplication* (denoted by ab or $a \cdot b$ or $a \times b$). We assume the following axioms about \mathbb{R} :

- Axiom 1.** (CLOSURE OF \mathbb{R}) If a and b are real numbers, then so are $a + b$ and ab .
- Axiom 2.** (COMMUTATIVITY) $a + b = b + a$ and $ab = ba$ for all real numbers a and b .
- Axiom 3.** (ASSOCIATIVITY) $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$ for all real numbers a , b , and c .
- Axiom 4.** (DISTRIBUTIVITY) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ for all real numbers a , b , and c .
- Axiom 5.** (IDENTITIES) There exist two distinct real numbers, denoted by 0 and 1, such $0 + a = a + 0 = a$ and $1 \cdot a = a \cdot 1 = a$ for every real number a .
- Axiom 6.** (ADDITIONAL INVERSES) For every real number a , there exists a real number $-a$, called the *additive inverse* or *opposite* of a , such that $a + (-a) = (-a) + a = 0$.
- Axiom 7.** (MULTIPLICATIVE INVERSES) For every nonzero real number a , there exists a real number a^{-1} , called the *multiplicative inverse* or *reciprocal* of a , such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Any set endowed with two operations satisfying these axioms is called a *field*, so our assumptions so far can be summarized by saying that \mathbb{R} is a field. (Can you think of any other fields?)

Based on these axioms, we can begin to prove some theorems. But first, some definitions. In all of these definitions, a and b represent arbitrary real numbers.

Definitions

- The numbers **2** through **10** are defined by $2 = 1 + 1$, $3 = 2 + 1$, etc. The decimal representations for other numbers are defined by the usual rules of decimal notation: For example, 23 is defined to be $2 \cdot 10 + 3$, etc.
- The **difference between a and b** , denoted by $a - b$, is the real number defined by $a - b = a + (-b)$, and is said to be obtained by **subtracting b from a** .
- If $b \neq 0$, the **quotient of a and b** , denoted by a/b , is the real number defined by $a/b = ab^{-1}$, and is said to be obtained by **dividing a by b** .
- The **square of a** , denoted by a^2 , is the number $a \cdot a$.

Theorems

These theorems can be proved from the axioms in the order listed below. In all of these theorems, a , b , c , d represent arbitrary real numbers.

Theorem 1. (CANCELLATION LAWS) If $a + c = b + c$, then $a = b$. If $ac = bc$ and $c \neq 0$, then $a = b$.

Theorem 2. (UNIQUENESS OF IDENTITIES) The numbers 0 and 1 in the identity axiom are unique.

Theorem 3. (UNIQUENESS OF INVERSES) For any a , the number $-a$ such that $a + (-a) = (-a) + a = 0$ is unique; and for any nonzero a , the number a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$ is unique.

Theorem 4. $-0 = 0$.

Theorem 5. $a - a = 0$.

Theorem 6. $a - 0 = a$.

Theorem 7. $0 - a = -a$.

Theorem 8. $-(-a) = a$.

Theorem 9. $0a = 0$.

Theorem 10. $-a = (-1)a$.

Theorem 11. $(-a)b = -(ab)$.

Theorem 12. $(-a)(-b) = ab$.

Theorem 13. $a(b - c) = ab - ac$.

Theorem 14. $-(a + b) = -a - b$.

Theorem 15. $-(a - b) = b - a$.

Theorem 16. $(a + b)(c + d) = ac + ad + bc + bd$.

Theorem 17. $1^{-1} = 1$.

Theorem 18. $a/1 = a$.

Theorem 19. If $a \neq 0$, then $a/a = 1$.

Theorem 20. If $a \neq 0$, then $a^{-1} \neq 0$.

Theorem 21. If $a \neq 0$, then $a^{-1} = 1/a$.

Theorem 22. If $a \neq 0$, then $(-a)^{-1} = -(1/a)$.

Theorem 23. If $a \neq 0$, then $(a^{-1})^{-1} = a$.

Theorem 24. If $ab = 0$, then $a = 0$ or $b = 0$.

Theorem 25. If $a \neq 0$ and $b \neq 0$, then $(ab)^{-1} = a^{-1}b^{-1}$.

Theorem 26. If $a \neq 0$ and $b \neq 0$, then $(a/b)^{-1} = b/a$.

Theorem 27. If $a^2 = b^2$, then $a = \pm b$.

Theorem 28. $a^2 = 0$ if and only if $a = 0$.

Theorem 29. $(-a)^2 = a^2$.

Theorem 30. $(a^{-1})^2 = 1/a^2$.

Theorem 31. If $b \neq 0$ and $d \neq 0$, then $(a/b)(c/d) = (ac)/(bd)$.

Theorem 32. If $b \neq 0$, $c \neq 0$, and $d \neq 0$, then $(a/b)/(c/d) = (ad)/(bc)$.

Theorem 33. If $c \neq 0$, then $(a/c) + (b/c) = (a + b)/c$.

Theorem 34. If $b \neq 0$ and $d \neq 0$, then $(a/b) + (c/d) = (ad + bc)/(bd)$.

GROUP II: ORDER AXIOMS

For our second group of axioms, we assume that there exists a subset $\mathbb{R}^+ \subseteq \mathbb{R}$ whose elements are called **positive real numbers**, such that the following statements are true.

Axiom 8. (CLOSURE OF \mathbb{R}^+) If a and b are positive real numbers, then so are $a + b$ and ab .

Axiom 9. (TRICHOTOMY AXIOM) If a is a real number, then one and only one of the following three statements is true: $a \in \mathbb{R}^+$, $-a \in \mathbb{R}^+$, or $a = 0$.

A field \mathbb{R} together with a subset \mathbb{R}^+ satisfying these two axioms is called an *ordered field*. So our axioms so far state that \mathbb{R} is an ordered field.

More Definitions

- a is less than b , denoted by $a < b$, means $b - a$ is positive.
- a is less than or equal to b , denoted by $a \leq b$, means $a < b$ or $a = b$.
- a is greater than b , denoted by $a > b$, means $b < a$.
- a is greater than or equal to b , denoted by $a \geq b$, means $a > b$ or $a = b$.
- A real number a is *negative* if $a < 0$.
- A real number a is *nonnegative* if $a \geq 0$.
- A real number a is *nonpositive* if $a \leq 0$.
- If S is a set of real numbers, a real number b is said to be the *largest element of S* or the *maximum of S* if b is an element of S and, in addition, $b \geq x$ whenever x is any element of S . The terms *smallest element* and *minimum* are defined similarly.
- The *absolute value of a* is the number $|a|$ defined by

$$|a| = \begin{cases} a, & a \geq 0, \\ -a, & a < 0. \end{cases}$$

More Theorems

Here are theorems about ordered fields. As before, these can be proved from the axioms in the order listed below. In all of these theorems, a, b, c, d represent arbitrary real numbers.

Theorem 35. (TRICHOTOMY LAW FOR INEQUALITIES) If a and b are real numbers, then one and only one of the following three statements is true: $a < b$, $a = b$, or $a > b$.

Theorem 36. (TRANSITIVE LAW) If $a < b$ and $b < c$, then $a < c$.

Theorem 36a. a is positive if and only if $a > 0$.

Theorem 37. If $a < b$, then $a + c < b + c$.

Theorem 38. If $a < c$ and $b < d$, then $a + b < c + d$.

Theorem 39. If $a < b$ and $c > 0$, then $ac < bc$.

Theorem 40. If $a < b$ and $c < 0$, then $ac > bc$.

Theorem 41. $a^2 > 0$ if and only if $a \neq 0$.

Theorem 42. $1 > 0$.

Theorem 43. If $a < b$ and a and b are both positive, then $a^2 < b^2$.

Theorem 44. If $a < b$ and a and b are both negative, then $a^2 > b^2$.

Theorem 45. If $a < b$, then $-a > -b$.

Theorem 46. $a > 0$ if and only if $-a < 0$.

Theorem 47. $ab > 0$ if and only if a and b are both positive or both negative.

Theorem 48. $ab < 0$ if and only if one is positive and the other is negative.

Theorem 49. $|a| = 0$ if and only if $a = 0$.

Theorem 50. $|a| > 0$ if and only if $a \neq 0$.

Theorem 51. $|a| \geq 0$.

Theorem 52. $a \leq |a|$.

Theorem 53. $|-a| = |a|$.

Theorem 54. $|a| = \max\{a, -a\}$.

Theorem 55. $|a^{-1}| = 1/|a|$ if $a \neq 0$.

Theorem 56. $|ab| = |a||b|$.

Theorem 57. $|a/b| = |a|/|b|$ if $b \neq 0$.

Theorem 58. If $|a| = |b|$, then $a = \pm b$.

Theorem 59. If a and b are both nonnegative, then $|a| \geq |b|$ if and only if $a \geq b$.

Theorem 60. If a and b are both negative, then $|a| \geq |b|$ if and only if $a \leq b$.

Theorem 61. $|a| < b$ if and only if $a > -b$ and $a < b$.

Theorem 62. $|a| > b$ if and only if $a < -b$ or $a > b$.

Theorem 63. (THE TRIANGLE INEQUALITY) $|a + b| \leq |a| + |b|$.

Theorem 64. (THE REVERSE TRIANGLE INEQUALITY) $||a| - |b|| \leq |a - b|$.

Theorem 65. (DENSITY OF REAL NUMBERS) If $a < b$, there exists a real number c such that $a < c < b$.

Theorem 66. There does not exist a smallest or largest real number.

Theorem 67. There does not exist a smallest positive real number.

GROUP III: LEAST UPPER BOUND AXIOM

One more axiom to go. Before we state it, we need a few more definitions.

More Definitions

- If S is a set of real numbers, a real number b (not necessarily in S) is said to be an *upper bound for S* if $b \geq x$ for every x in S . A *lower bound* is defined similarly.
- If S is a set of real numbers, a real number b (not necessarily in S) is said to be a *least upper bound for S* if it is an upper bound, and in addition every other upper bound b' for S satisfies $b' \geq b$. A *greatest lower bound* is defined similarly.

Axiom 10. (THE LEAST UPPER BOUND AXIOM) Every nonempty set of real numbers that has an upper bound has a least upper bound.

An ordered field satisfying the least upper bound axiom is said to be *complete*. So now we can summarize our entire set of assumptions about the real numbers:

There exists a complete ordered field \mathbb{R} .

And a Few More Theorems

Theorem 68. If a is any nonnegative real number, there is a unique nonnegative real number \sqrt{a} such that $(\sqrt{a})^2 = a$.

Theorem 69. If $a^2 = b$, then $a = \pm\sqrt{b}$.

Theorem 70. $\sqrt{a^2} = |a|$.

Theorem 71. If $a < b$ and a and b are both nonnegative, then $\sqrt{a} < \sqrt{b}$.