

# Comprehensive Review of MTH 331

Joe White

December 10, 2025

---

## 1 Sets and Basic Set Operations

A *set* is simply a collection of objects, which we call *elements* of the set. If an object  $x$  belongs to a set  $A$ , we write  $x \in A$ , which can be read as “ $x$  is in the set  $A$ ”. Objects do not need to be numbers; they can be symbols, functions, or even other sets. For example,  $\{1, \{2, 3\}, 7\}$  is a set whose second element is itself a set.

A common way to list the elements of a finite set is with curly braces. For example,

$$X = \{a, b, c\}$$

is the set whose elements are  $a$ ,  $b$ , and  $c$ . Another useful notation is *set-builder notation*:

$$\{x \mid P(x)\},$$

which denotes the set of all objects  $x$  for which the statement  $P(x)$  is true. For instance,

$$\{n \in \mathbb{N} \mid n \text{ is even}\}$$

is the set of even natural numbers.

One of the most basic principles of set theory is the *axiom of extensionality*. It states that two sets are equal if and only if they have exactly the same elements. In symbols, if

$$\forall x, (x \in A \iff x \in B),$$

then  $A = B$ . This tells us that sets are completely determined by their elements, not by the order in which we write them or how we define them.

We say  $A$  is a *subset* of  $B$  if every element of  $A$  is also an element of  $B$ :

$$A \subseteq B \quad \text{means} \quad (\forall x)(x \in A \implies x \in B).$$

If  $A \subseteq B$  but  $A \neq B$ , then  $A$  is a *proper* subset of  $B$ . For example,  $\{1, 3\} \subseteq \{1, 2, 3, 4\}$ .

There are three standard operations on sets:

$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$	(union)
$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$	(intersection)
$A - B = \{x \mid x \in A \text{ and } x \notin B\}$	(set difference).

For example, if  $A = \{1, 2, 3\}$  and  $B = \{3, 4\}$ , then  $A \cup B = \{1, 2, 3, 4\}$ ,  $A \cap B = \{3\}$ , and  $A - B = \{1, 2\}$ .

Not every expression of the form  $\{x \mid P(x)\}$  actually defines a set. A famous example is *Russell's paradox*. Suppose we try to form the set

$$R = \{x \mid x \text{ is a set and } x \notin x\}.$$

If  $R \in R$ , then by definition  $R \notin R$ , a contradiction. But if  $R \notin R$ , then it satisfies its own defining property and so  $R \in R$ , again a contradiction. This shows that no such set  $R$  can exist.

## 2 Natural Numbers and Mathematical Induction

We usually think of the natural numbers as the list

$$\mathbb{N} = \{0, 1, 2, \dots\},$$

but in set theory it is useful to give a more precise definition. One approach, due to John von Neumann, is to define each natural number as the set of all smaller natural numbers. In this construction,

$$0 = \emptyset, \quad 1 = \{0\} = \{\emptyset\}, \quad 2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\},$$

and in general,

$$n = \{0, 1, 2, \dots, n-1\}.$$

With this definition, the next number is obtained simply by adding one new element:

$$n+1 = n \cup \{n\}.$$

This viewpoint is surprisingly useful, because it treats numbers and sets in a unified way. For example,  $2 \in 4$  becomes literally true, since 2 is one of the elements of the set  $\{0, 1, 2, 3\}$ .

To define  $\mathbb{N}$  itself, we introduce the idea of an *inductive* set. A set  $S$  is inductive if:

- (1)  $0 \in S$ , and
- (2) whenever  $x \in S$ , then  $x+1 \in S$ .

The set  $\mathbb{N}$  should certainly be inductive, but there are other inductive sets that contain additional elements. To capture only the intended natural numbers, we define:

$$\mathbb{N} = \{x \mid x \text{ belongs to every inductive set}\}.$$

This definition ensures that  $\mathbb{N}$  contains exactly the numbers that can be reached starting from 0 and repeatedly adding 1, and nothing extra.

The precise construction of  $\mathbb{N}$  using inductive sets is also what allows us to justify the method of *mathematical induction*. A typical induction proof shows that a statement  $P(n)$  holds for all natural numbers by:

- (1) proving the base case  $P(0)$  (or sometimes  $P(1)$ ), and
- (2) showing that whenever  $P(n)$  is true, the statement  $P(n+1)$  is also true.

If a set of natural numbers satisfies these two properties, then it is inductive. Since  $\mathbb{N}$  is defined to be the smallest inductive set, it follows that every natural number must satisfy  $P(n)$ . This is why induction works.

### 3 Ordered Pairs, Relations, and Functions

Sets themselves do not have any notion of order: for example,

$$\{1, 2\} = \{2, 1\}.$$

However, in mathematics we often need to keep track of order, especially when defining coordinates, functions, and relations. One way to build ordered pairs using only sets is due to Kazimierz Kuratowski, who defined

$$(x, y) = \{\{x\}, \{x, y\}\}.$$

This construction behaves exactly like an ordered pair should. In particular, if

$$(x, y) = (a, b),$$

then the two sets  $\{\{x\}, \{x, y\}\}$  and  $\{\{a\}, \{a, b\}\}$  must be equal. Because sets are determined entirely by their elements, this equality forces  $x = a$  and  $y = b$ , so order is preserved even though the underlying objects are sets.

Using ordered pairs, we can define the *Cartesian product* of two sets:

$$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}.$$

A *relation* from  $A$  to  $B$  is any subset of  $A \times B$ . For example, if

$$A = \{1, 2, 3\}, \quad B = \{a, b\},$$

then

$$R = \{(1, a), (2, a), (3, b)\}$$

is a relation from  $A$  to  $B$ .

A *function* from  $A$  to  $B$  is a special kind of relation with two properties:

- (1) For every  $x \in A$ , there exists  $y \in B$  such that  $(x, y) \in f$ .
- (2) If  $(x, y_1)$  and  $(x, y_2)$  are both in  $f$ , then  $y_1 = y_2$ .

If  $(x, y) \in f$ , we usually write  $f(x) = y$ . In plain English, a function assigns to each element of  $A$  *exactly one* element of  $B$ .

We often want to describe how completely a function reaches its codomain or how distinctly it treats its inputs. This leads to three important properties.

**Surjective.** A function  $f : A \rightarrow B$  is *surjective* (onto) if every element of  $B$  is the output of at least one element of  $A$ :

$$(\forall y \in B)(\exists x \in A)(f(x) = y).$$

Example:  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  defined by  $f(x) = x - 1$  is surjective, since every integer  $y$  is  $f(y + 1)$ .

**Injective.** A function  $f : A \rightarrow B$  is *injective* (one-to-one) if different inputs always have different outputs:

$$f(x_1) = f(x_2) \implies x_1 = x_2.$$

Example:  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  defined by  $f(x) = 2x$  is injective. Nonexample:  $g(x) = x^2$  is not injective on  $\mathbb{Z}$  since  $g(2) = g(-2)$ .

**Bijjective.** A *bijection* is both injective and surjective. These functions match elements of  $A$  and  $B$  in a perfect one-to-one correspondence, so they show that  $A$  and  $B$  have the same cardinality. For example,  $f : \mathbb{N} \rightarrow \mathbb{N} \setminus \{0\}$  defined by  $f(n) = n + 1$  is a bijection.

## 4 Properties of Relations on a Set

A relation on a set  $A$  is simply a subset of the Cartesian product  $A \times A$ . Thus a relation  $R$  on  $A$  is a set of ordered pairs  $(x, y)$  with  $x, y \in A$ . When  $(x, y) \in R$ , we also write  $xRy$ . For example, the “less than or equal to” relation on  $\mathbb{N}$  can be written formally as

$$\{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}.$$

In roster notation, this begins as

$$\{(0, 0), (0, 1), (0, 2), \dots, (1, 1), (1, 2), (1, 3), \dots, (2, 2), (2, 3), \dots\},$$

listing all pairs whose first coordinate is less than or equal to the second.

Given a relation  $R$  on a set  $A$ , some basic properties are:

- **Reflexive:** For all  $x \in A$ ,  $xRx$ . Every element is related to itself. Negation: there exists  $x \in A$  such that  $x \not Rx$ .
- **Symmetric:** For all  $x, y \in A$ ,  $xRy \implies yRx$ . The relation works in both directions. Negation: there exist  $x, y$  with  $xRy$  but  $y \not Rx$ .
- **Antisymmetric:** For all  $x, y \in A$ , if  $xRy$  and  $yRx$ , then  $x = y$ . The only way two elements can relate in both directions is if they are equal. Negation: there exist  $x \neq y$  with  $xRy$  and  $yRx$ .
- **Transitive:** For all  $x, y, z \in A$ ,  $xRy$  and  $yRz$  imply  $xRz$ . The relation passes through intermediate elements. Negation: there exist  $x, y, z$  with  $xRy$  and  $yRz$  but  $x \not Rz$ .
- **Total:** For all  $x, y \in A$ , at least one of  $xRy$  or  $yRx$  holds. Every pair of elements is comparable. Negation: there exist  $x, y \in A$  with neither  $xRy$  nor  $yRx$ .

Here are some examples:

- **Equality on any set  $A$ :** The relation  $x = y$  is reflexive, symmetric, antisymmetric, transitive, and total.

- **Divisibility on  $\mathbb{N}$ :**  $x \mid y$  means there exists  $k \in \mathbb{N}$  with  $y = kx$ . This relation is reflexive (since  $x = 1 \cdot x$ ), transitive, and antisymmetric, but it is not symmetric ( $2 \mid 4$  but  $4 \nmid 2$ ). It is also not total, since  $2 \nmid 3$  and  $3 \nmid 2$ .
- **Less-than relation  $<$  on  $\mathbb{N}$ :** This relation is transitive and irreflexive ( $x \not< x$ ), but not symmetric and not total.
- **A relation given by listing pairs:** Let  $A = \{1, 2, 3\}$  and

$$R = \{(1, 1), (1, 2), (2, 2), (3, 1)\}.$$

This relation is reflexive for 1 and 2 but not for 3; symmetric only for the pair (2, 2); anti-symmetric; not transitive; and not total because (2, 3) and (3, 2) are both missing.

These examples illustrate how relations can behave very differently depending on their structure.

## 5 Partial Orderings, Total Orderings, and Well-Orderings

A *partial ordering* on a set  $A$  is a relation on  $A$  that is reflexive, antisymmetric, and transitive.

For example, the subset relation is a partial ordering. Let  $A$  be any collection of sets, and consider the relation  $\subseteq$  on  $A$  defined by  $X \subseteq Y$ .

- Reflexive: Every set is a subset of itself, so  $X \subseteq X$ .
- Antisymmetric: If  $X \subseteq Y$  and  $Y \subseteq X$ , then  $X = Y$ .
- Transitive: If  $X \subseteq Y$  and  $Y \subseteq Z$ , then  $X \subseteq Z$ .

Thus  $\subseteq$  is a partial ordering. It is not total, because for example  $\{1\}$  and  $\{2\}$  are not comparable by  $\subseteq$ .

Another example is divisibility on  $\mathbb{N}$ . Let  $A$  be a set of positive integers, and define  $x \mid y$  to mean that  $y = kx$  for some  $k \in \mathbb{Z}$ .

- Reflexive:  $x \mid x$ , since  $x = 1 \cdot x$ .
- Antisymmetric: If  $x \mid y$  and  $y \mid x$ , then  $x = ky$  and  $y = \ell x$  for some integers  $k, \ell$ . Substituting gives  $x = k\ell x$ , so  $k\ell = 1$ . Since  $x$  and  $y$  are positive, this forces  $k = \ell = 1$ , hence  $x = y$ .
- Transitive: If  $x \mid y$  and  $y \mid z$ , then  $y = kx$  and  $z = \ell y = \ell kx$ , so  $x \mid z$ .

Thus divisibility is a partial ordering on the positive integers. However, on the whole set  $\mathbb{Z}$  it is not antisymmetric: for instance,  $2 \mid -2$  and  $-2 \mid 2$ , but  $2 \neq -2$ . So divisibility is not a partial order on all integers. Divisibility is also not total, for example,  $2 \nmid 3$  and  $3 \nmid 2$ .

The relation  $\leq$  on the real numbers is both a partial and a total ordering. On any set of real numbers  $A$ , the relation  $\leq$  is reflexive, antisymmetric, and transitive. It is also total, because for any real numbers  $x$  and  $y$ , either  $x \leq y$  or  $y \leq x$ . Thus  $\leq$  is not only a partial ordering, it is a total ordering.

In general, a relation on  $A$  is a *total ordering* if it is reflexive, antisymmetric, transitive, and total. The examples above show that:

- $\leq$  on  $\mathbb{R}$  is a total ordering,
- $\subseteq$  on a collection of sets is not total,
- divisibility on  $\mathbb{N}$  is not total.

A total ordering is called a *well-ordering* if every nonempty subset has a least element. For example:

- The usual order  $\leq$  on  $\mathbb{N}$  is a well-ordering.
- The usual order on  $\mathbb{Z}$  is not a well-ordering, because  $\mathbb{Z}$  has subsets with no least element (for example, all negative integers).
- The usual order on  $\mathbb{R}$  is not a well-ordering, since  $(0, 1)$  has no least element.

Well-orderings are important in the study of induction, infinite sets, and ordinal numbers.

## 6 Equivalence Relations and Partitions

An *equivalence relation* on  $A$  is a relation on  $A$  that is reflexive, symmetric, and transitive.

A basic example is equality: the relation

$$R = \{(x, y) \in A \times A \mid x = y\}$$

is an equivalence relation on  $A$ . Another extreme example is  $R = A \times A$ , where every pair of elements is related; this is also an equivalence relation.

If  $R$  is an equivalence relation on a set  $A$  and  $a \in A$ , the *equivalence class* of  $a$  is

$$[a] = \{x \in A \mid xRa\}.$$

Two key facts are:

- $[a] = [b]$  if and only if  $aRb$ .
- If  $[a] \neq [b]$ , then  $[a] \cap [b] = \emptyset$ .

The set of all equivalence classes,

$$\{[a] \mid a \in A\},$$

forms a *partition* of  $A$ , meaning that the classes are nonempty, pairwise disjoint, and their union is  $A$ .

For a fixed positive integer  $n$ , the relation of congruence mod  $n$  is an important example. For integers  $x$  and  $y$ , we say

$$x \equiv y \pmod{n}$$

if  $n \mid (x - y)$ . This is an equivalence relation on  $\mathbb{Z}$ . Its equivalence classes are the sets

$$[0], [1], \dots, [n-1],$$

where, for example,

$$[1] = \{\dots, -2n+1, -n+1, 1, n+1, 2n+1, \dots\}.$$

If  $a \equiv a' \pmod{n}$  and  $b \equiv b' \pmod{n}$ , then

$$a + b \equiv a' + b' \pmod{n} \quad \text{and} \quad ab \equiv a'b' \pmod{n}.$$

This means that the operations

$$[a] + [b] = [a + b] \quad \text{and} \quad [a] \cdot [b] = [ab]$$

are well-defined on equivalence classes modulo  $n$ .

However, the operation  $[a]^{[b]} = [a^b]$  is not well-defined on equivalence classes mod  $n$ , since choosing different representatives of the same class can change the value of  $a^b$  modulo  $n$ .

## 7 Even and Odd Integers, and the Irrationality of $\sqrt{2}$

An integer  $n$  is called *even* if there exists an integer  $k$  such that  $n = 2k$ . Similarly,  $n$  is called *odd* if  $n = 2k + 1$  for some integer  $k$ . These two possibilities cover all integers, and a number can never be both even and odd.

To see this, let  $n$  be any integer. When  $n$  is divided by 2, the division algorithm guarantees that

$$n = 2k \quad \text{or} \quad n = 2k + 1$$

for some integer  $k$ . The first case means  $n$  is even, and the second means  $n$  is odd. They cannot both occur: if  $2k = 2m + 1$ , then  $2(k - m) = 1$ , which is impossible since the left-hand side is even.

An important fact about odd numbers is as follows. If  $a$  and  $b$  are odd, then  $a = 2m + 1$  and  $b = 2n + 1$  for some integers  $m, n$ . Multiplying gives

$$ab = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1,$$

so  $ab$  is also of the form  $2k + 1$ . Thus:

The product of two odd numbers is odd.

A very useful consequence is the contrapositive:

If  $ab$  is even, then at least one of  $a$  or  $b$  is even.

Taking  $a = b = n$  gives an important special case:

If  $n^2$  is even, then  $n$  must be even.

This observation helps prove the following result:  $\sqrt{2}$  is irrational. Suppose instead that  $\sqrt{2}$  were rational. Then it could be written as a fraction in lowest terms,

$$\sqrt{2} = \frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad b \neq 0, \quad \gcd(a, b) = 1.$$

Squaring both sides gives

$$2 = \frac{a^2}{b^2} \implies a^2 = 2b^2.$$

Thus  $a^2$  is even, which means  $a$  is even. Write  $a = 2k$ . Then

$$(2k)^2 = 2b^2 \implies 4k^2 = 2b^2 \implies b^2 = 2k^2,$$

so  $b^2$  is even, and therefore  $b$  is even as well.

But if both  $a$  and  $b$  are even, then  $\frac{a}{b}$  was not in lowest terms, a contradiction. Thus no such fraction exists, and  $\sqrt{2}$  is irrational.

This argument can also be phrased using the method of least counterexample. Assume there is a rational number equal to  $\sqrt{2}$  and choose one with the smallest possible denominator. The same reasoning above forces both numerator and denominator to be even, contradicting minimality. Either form of the argument establishes the irrationality of  $\sqrt{2}$ .

## 8 Prime Numbers, Euclid's Lemma, and the Irrationality of $\sqrt{p}$

An integer  $n > 1$  is called *composite* if it can be written in the form

$$n = ab$$

for some integers  $a, b > 1$ . If an integer  $n > 1$  is not composite, then it is called *prime*. Thus a prime number has no positive divisors other than 1 and itself.

A fundamental fact about prime numbers is *Euclid's lemma*:

**Euclid's Lemma.** If  $p$  is prime and  $p \mid ab$ , then  $p \mid a$  or  $p \mid b$ .

One simple but important special case is obtained by taking  $a = b = n$ . If  $p \mid n^2$ , then Euclid's lemma tells us that  $p \mid n$ . In the case of  $p = 2$ , this means: if  $n^2$  is even, then  $n$  must be even.

Euclid's lemma makes it straightforward to prove that  $\sqrt{p}$  is irrational for every prime  $p$ . The argument is a direct generalization of the proof that  $\sqrt{2}$  is irrational.

**Theorem.** If  $p$  is prime, then  $\sqrt{p}$  is irrational.

**Proof.** Suppose, toward a contradiction, that  $\sqrt{p}$  is rational. Then it can be written in lowest terms as

$$\sqrt{p} = \frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad b \neq 0, \quad \gcd(a, b) = 1.$$

Squaring both sides gives

$$p = \frac{a^2}{b^2} \implies a^2 = pb^2.$$

Thus  $p \mid a^2$ , and by Euclid's lemma we conclude that  $p \mid a$ . So  $a = pk$  for some integer  $k$ . Substituting this into the equation gives

$$pb^2 = a^2 = (pk)^2 = p^2k^2,$$

so

$$b^2 = pk^2.$$

Hence  $p \mid b^2$ , and again by Euclid's lemma,  $p \mid b$ .

Therefore both  $a$  and  $b$  are divisible by  $p$ , contradicting the assumption that  $a/b$  was written in lowest terms. Thus no such fraction exists, and  $\sqrt{p}$  is irrational.  $\square$

Euclid's lemma is also a key ingredient in the Fundamental Theorem of Arithmetic, which states that every integer greater than 1 has a unique prime factorization.

## 9 Finite, Countably Infinite, and Uncountable Sets

A set  $A$  is *finite* if there exists a natural number  $n$  and distinct elements  $a_0, a_1, \dots, a_{n-1}$  of  $A$  such that

$$A = \{a_0, a_1, \dots, a_{n-1}\}.$$

In this case we say  $A$  has *cardinality*  $n$  and write  $|A| = n$ . Since  $n$  itself can be realized as the set  $\{0, 1, \dots, n-1\}$ , we obtain a bijection  $f : n \rightarrow A$  by defining  $f(k) = a_k$ . Thus a finite set is precisely one that can be put into bijection with some initial segment of the natural numbers.

A set  $A$  is *countably infinite* if its elements can be listed in an infinite sequence:

$$A = \{a_0, a_1, a_2, \dots\},$$

with all  $a_k$  distinct. Defining  $f(k) = a_k$  gives a bijection  $f : \mathbb{N} \rightarrow A$ . This is the formal way of saying that the elements of  $A$  can be “counted” using the natural numbers.

The set  $\mathbb{N}$  itself is countably infinite. Another standard example is  $\mathbb{Z}$ . One way to see this is to list the integers in the order

$$0, 1, -1, 2, -2, 3, -3, \dots$$

and define  $f : \mathbb{N} \rightarrow \mathbb{Z}$  by

$$f(0) = 0, \quad f(2k-1) = k, \quad f(2k) = -k \quad (k \geq 1).$$

This is a bijection, so  $\mathbb{Z}$  is countably infinite.

If  $A$  is countably infinite, then there is always an injective function from  $A$  to itself that is not surjective. For example, for  $A = \mathbb{N}$ , the function  $f : \mathbb{N} \rightarrow \mathbb{N}$  defined by  $f(k) = k + 1$  is injective (different inputs have different outputs), but not surjective, since 0 is not in its range. More generally, if  $A = \{a_0, a_1, a_2, \dots\}$ , the function  $g : A \rightarrow A$  defined by  $g(a_k) = a_{k+1}$  is injective but not surjective (since  $a_0$  is not in the range).

By contrast, if  $A$  is finite, then every injective function  $f : A \rightarrow A$  is automatically surjective. One way to see this is by induction on  $|A|$ . This distinction motivates an important characterization: a set is *infinite* if and only if it has the same cardinality as a proper subset of itself.

A set is called *uncountable* if it is infinite but not countably infinite. Georg Cantor showed that the real numbers  $\mathbb{R}$  are uncountable. That is, there is no way to list all real numbers in a sequence  $r_0, r_1, r_2, \dots$  so that every real number appears somewhere on the list.

The set of rational numbers  $\mathbb{Q}$ , on the other hand, is countably infinite. Every rational number can be written as a reduced fraction  $a/b$  with  $a \in \mathbb{Z}$  and  $b \in \mathbb{N}$ , and these pairs  $(a, b)$  can be listed systematically. Removing duplicates yields a bijection from  $\mathbb{N}$  to  $\mathbb{Q}$ .

We can use these ideas to see that most real numbers are irrational. Consider the set of irrational numbers  $\mathbb{R} \setminus \mathbb{Q}$ . We claim this set is uncountable.

Suppose, toward a contradiction, that  $\mathbb{R} \setminus \mathbb{Q}$  were countably infinite. Then both  $\mathbb{Q}$  and  $\mathbb{R} \setminus \mathbb{Q}$  would be countably infinite sets. Since these two sets are disjoint and their union is all of  $\mathbb{R}$ , we would have

$$\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$$

as the union of two countably infinite sets.

But the union of any two disjoint countably infinite sets is again countably infinite: if  $A = \{a_0, a_1, a_2, \dots\}$  and  $B = \{b_0, b_1, b_2, \dots\}$ , then the alternating sequence

$$a_0, b_0, a_1, b_1, a_2, b_2, \dots$$

lists every element of  $A \cup B$  exactly once. Thus  $\mathbb{R}$  would be countably infinite, contradicting Cantor's theorem. Therefore,  $\mathbb{R} \setminus \mathbb{Q}$  must be uncountable.

This justifies the intuitive statement that “most real numbers are irrational”: the irrational numbers form an uncountable set, whereas the rational numbers form only a countably infinite subset.