Chapter 4

Sets of Real Numbers

4.1 The Integers $\mathbb{Z}$ and their Properties

In our previous discussions about sets and functions, the set of integers $\mathbb{Z}$ served as a key example. Its ubiquitousness comes from the fact that integers and their properties are well-known to mathematicians and non-mathematicians. In this section, we will investigate in more detail what aspects of integer arithmetic make it so useful.

4.1.1 Arithmetic Properties of $\mathbb{Z}$

Recall that as a set, the integers $\mathbb{Z}$ are all whole numbers, positive, negative, and zero:

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

The true power of the integers, though, comes from its arithmetic structure. In particular, $\mathbb{Z}$ enjoys the following obvious, yet important, algebraic properties:

- *Closed under Addition:* If $m, n \in \mathbb{Z}$, then $m + n \in \mathbb{Z}$. In other words, if m and n are integers, then their sum $m + n$ is also an integer.

- *Closed under Additive Inverses:* If $m \in \mathbb{Z}$, then there exists another integer (namely, $-m \in \mathbb{Z}$) such that $m + (-m) = 0$.

- *Closed under Multiplication:* If $m, n \in \mathbb{Z}$, then $m \cdot n \in \mathbb{Z}$. In other words, if m and n are integers, then their product $m \cdot n$ is also an integer.

- *Distributive Property:* If $m, n, l \in \mathbb{Z}$, then

  $$m \cdot (n + l) = m \cdot n + m \cdot l.$$

  In other words, the two operations of multiplication and addition behave nicely together.

The above properties of $\mathbb{Z}$, as obvious as they are, indicate that the algebraic structure of $\mathbb{Z}$ is particularly nice. In fact, these properties, along with other technical ones, make the integers $\mathbb{Z}$ into what algebraists call a *ring*.

Notice that we did not include the property "Closed Under Multiplicative Inverses." The reason for this is simply because $\mathbb{Z}$ fails to have this property. In other words, if $m \in \mathbb{Z}$ and $m \neq 0$, we can ask if there exists an integer $m^{-1} \in \mathbb{Z}$ such that $m \cdot m^{-1} = 1$. This rarely happens. For example, $3 \in \mathbb{Z}$ has no multiplicative inverse since the only real number that can multiply with 3 to produce 1 is $\frac{1}{3} \notin \mathbb{Z}$, which is not an integer. In fact, the only integers whose multiplicative inverses are also integers are 1 and -1. Thus, division is rare in the ring of integers; however, we will see that there is still a way to speak of *divisibility* of integers.

4.1.2 Divisibility of Integers

Integers can be broken up into two disjoint subsets: the set of even integers and the set of odd integers. More specifically, we say that a number $n \in \mathbb{Z}$ is **even** if there exists an integer $k \in \mathbb{Z}$ such that $n = 2k$. Key to this definition is that k is indeed a whole number. An integer m which is not even is called **odd** and can be written as $m = 2k + 1$ for some $k \in \mathbb{Z}$.

In previous sections, we proved some simple propositions about even and odd numbers and saw that they boiled down to being able to write a number in a certain form. Here, we wish to generalize the concept of an even number to the broader concept of *divisibility*.

Another way to phrase the definition of an even number is to say that n is divisible by 2; equivalently, we can say that 2 divides n. In general, we can say that an integer m **divides** n if there exists an integer $k \in \mathbb{Z}$ such that $n = mk$. If m divides n, then this frequently notated by

$$m|n.$$

Since the definition of divisibility is in the form of a "there exists" statement, we will be using much of the logic and previously developed techniques in our proofs.

Below are some examples of divisibility statements and associated proofs or counterexamples.

- We previously proved that n is even if and only if n^2 is even. We can re-write this in terms of divisibility as "$2|n$ if and only if $2|n^2$."

- We previous proved that if $m \cdot n$ is odd, then m and n are both odd. Since a whole number is odd if and only if it is not even, we can use the *does not divide* symbol $\nmid$ to re-write our statement as "If $2 \nmid m \cdot n$, then $2 \nmid n$ and $2 \nmid m$."

- Consider the statement

  $$\text{“if } a \mid b \text{ and } b \mid c\text{, then } a \mid c\text{.”}$$

  We can prove this statement rather easily. Since $a \mid b$ and $b \mid c$, then there exists integers $k_1, k_2 \in \mathbb{Z}$ such that $b = k_1 a$ and $c = k_2 b$. Substituting, we get that

  $$c = k_2 b = k_2(k_1 a) = (k_2 \cdot k_1)a.$$

  Since $k_1, k_2 \in \mathbb{Z}$, their product $k_2 k_1$ is also an integer. Thus, since $c = (k_2 k_1)a$, then c is written as a multiple of a and thus $a \mid c$.

- Consider the statement

  $$\text{“if } a \mid c \text{ and } b \mid d\text{, then } ab \mid cd\text{.”}$$

  This statement is true. Since $a \mid c$ and $b \mid d$, there exist integers $k_1, k_2 \in \mathbb{Z}$ such that $c = k_1 a$ and $d = k_2 b$. Thus,

  $$cd = (k_1 a)(k_2 b) = (k_1 k_2)ab.$$

  Since $k_1, k_2 \in \mathbb{Z}$, then $k_1 k_2 \in \mathbb{Z}$. Thus, $ab \mid cd$.

- Consider the statement

  "If $a \mid b$ and $a \mid c$, then $a \mid bx + cy$ for any integers $x, y \in \mathbb{Z}$."

  We will provide a proof for this statement. Sine $a \mid b$ and $a \mid c$, there exists integers $k_1, k_2 \in \mathbb{Z}$ such that $b = k_1 a$ and $c = k_2 a$. Thus,

  $$bx + cy = (k_1 a)x + (k_2 a)y = a(k_1 x + k_2 y).$$

  Since $x, y, k_1, k_2 \in \mathbb{Z}$, then $k_1 x + k_2 y \in \mathbb{Z}$ and thus $a \mid bx + cy$. Notice that this statement includes the statement "If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$" if we let $x = y = 1$.

- Consider the statement

  "if $a \mid b$ or $a \mid c$, then $a \mid bc$."

  We can also prove this statement rather easily. First, we can assume, *without loss of generality*, that $a \mid b$ (since the case $a \mid c$ is almost identical). Then, $b = ka$ for some $k \in \mathbb{Z}$. Thus, $bc = kac = (kc)a$. Since $k, c \in \mathbb{Z}$, then $kc \in \mathbb{Z}$ and thus $a \mid bc$.

- We can investigate the converse of the above statement as well:

  "If $a \mid bc$, then $a \mid b$ or $a \mid c$."

  We provide a counter-example showing that the above statement is not generally true. Consider $a = 4, b = 2$, and $c = 6$. Then, $a \mid bc$ is $4 \mid 2 \cdot 6 = 12$, a true statement. However, neither $4 \mid 2$ nor $4 \mid 6$ is true. The above statement is true under certain conditions on a (namely, when a is prime), but this proof is slightly out of the scope of these notes.

4.1.3 Divisibility Proofs

The divisibility proofs above were fairly straightforward because they simply used the definition of divisibility. For all of them, when we knew that $m \mid n$, then we always wrote "there exists a $k \in \mathbb{Z}$ such that $n = mk$." When we were asked to prove that $m \mid n$, then our job was to find some integer x such that $m = nx$, where usually x was some combination of the previous constants. Furthermore, we always included a sentence that showed that x was indeed an integers by invoking the fact that $\mathbb{Z}$ is closed under addition and multiplication.

Here, we will investigate some more complicated divisibility proofs that require some key observations. To begin, notice that we had previously mentioned that an integer m is odd if it is not even or, equivalently, that $m = 2k + 1$ for some $k \in \mathbb{Z}$. We can make similar statements in general. If $n \mid m$, then $m = nk$ for some $k \in \mathbb{Z}$; however, can we say anything about what happens when $n \nmid m$ (when n *does not divide* m)?

To answer the above question, we will take the example of $3 \nmid m$. Since $3 \nmid m$, we cannot write m as an integer multiple of 3. Written in a slightly odd way, we can say that it is not true that $m = 3k + 0$ for any $k \in \mathbb{Z}$. If we replace the 0 with any other multiple of 3, the the above statement is still not true. To make it true, we can simply replace 0 with any number that is *not divisible* by 3. Thus, if $3 \nmid m$, then either $m = 3k + 1$ or $m = 3k + 2$. Notice that replacing the 1 or 2 in the above statements with another number not divisible by 3 will reduce to one of the above two cases.

In general, if $n \nmid m$, then we can write m in one of the following firms:

$$m = nk + 1$$

$$m = nk + 2$$

$$\vdots$$

$$m = nk + (n-1)$$

for some $k \in \mathbb{Z}$. In the proof-writing context, this means that if we know that $n \nmid m$, then we can use a proof by cases. In fact, there will be a total of $n-1$ cases. We give an example of such a proof below.

Proposition. Let $a \in \mathbb{Z}$. If $3 \nmid a^2 - 1$, then $3 \mid a$.

Discussion. This proposition asks us to prove "If $3 \nmid a^2 - 1$, then $3 \mid a$." Thus, we have a conditional statement $p \Rightarrow q$ with p being "$3 \nmid a^2 - 1$" and q being "$3 \mid a$." We will instead prove its contrapositive $\neg q \Rightarrow \neg p$ given by "If $3 \nmid a$, then $3 \mid a^2 - 1$." Of course, the contrapositive also has a "does not divide" statement, but $3 \nmid a$ is easier to work with than $3 \nmid a^2 - 1$.

`What we know:` $3 \nmid a$. Thus, by the above arguments, we know that for some $k \in \mathbb{Z}$, $a = 3k + 1$ or $a = 3k + 2$.

`What we want:` $3 \mid a^2 - 1$. Thus, we need to write $a^2 - 1$ as $a^2 - 1 = 3x$ for some $x \in \mathbb{Z}$.

`What we'll do:` We will use the following two cases: $a = 3k + 1$ or $a = 3k + 2$. In both cases, we will use algebra to write $a^2 - 1$ as $3x$ for some $x \in \mathbb{Z}$. We will also be sure to note that our x is indeed an integer using properties of $\mathbb{Z}$.

Proof. We will instead prove the contrapositive of our statement: "If $3 \nmid a$, then $3 \mid a^2 - 1$."

Since $3 \nmid a$, then for some $k \in \mathbb{Z}$, we know that $a = 3k + 1$ or $a = 3k + 2$, leaving us with two cases. In the first case, $a = 3k + 1$. Thus,

$$a^2 - 1 = (3k+1)^2 - 1 = (9k^2 + 6k + 1) - 1 =$$

$$9k^2 + 6k = 3(3k^2 + 2k).$$

Since $k \in \mathbb{Z}$, then $3k^2 + 2k \in \mathbb{Z}$. Thus, $a^2 - 1 = 3(3k^2 + 2k)$ and $3 \mid a^2 - 1$, as desired.

In the second case, $a = 3k + 2$. Thus,

$$a^2 - 1 = (3k+2)^2 - 1 = (9k^2 + 12k + 4) - 1 =$$

$$9k^2 + 12k + 3 = 3(3k^2 + 4k + 1).$$

Since $k \in \mathbb{Z}$, then $3k^2 + 4k + 1 \in \mathbb{Z}$. Thus, $a^2 - 1 = 3(3k^2 + 4k + 1)$ and $3 \mid a^2 - 1$, as desired.

In either case, we conclude that $3 \mid a^2 - 1$. Thus, we have proven the contrapositive statement and the original statement "If $3 \nmid a^2 - 1$, then $3 \mid a$" is true.

$\square$

It is important to note that the converse of the above observation is true as well. That is, if we are trying to prove, for example, that $3 \nmid m$, and we are able to write $m = 3x + 1$ or $m = 3x + 2$ for some $x \in \mathbb{Z}$, then we are allowed to conclude that, in fact $3 \nmid m$.

4.2 Rational and Irrational Numbers

When studying the integers $\mathbb{Z}$, we noted that, although it has all of the important algebraic structure that makes it a ring (closed under addition, multiplication, and additive inverses), it does not have the property that it is *closed under multiplicative inverses*. In other words, division in the set of integers is not a possibility. In fact, we noted that if you consider $3 \in \mathbb{Z}$, that there is no other integer a such that $3 \cdot a = 1$.

4.2.1 The Rationals as a Field

In this section, we will investigate $\mathbb{Q}$, the set of rational numbers. Recall that the rationals are given in set-builder notation by

$$\mathbb{Q} = \left\{ \frac{p}{q} \,\middle|\, p, q \in \mathbb{Z}, q \neq 0 \right\}$$

with the added proviso that two rationals $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ are equal if $p_1 q_2 = p_2 q_1$.

If we re-consider our above example, this time viewing 3 as a rational number, then we can note that there does indeed indeed exist a multiplicative inverse, $\frac{1}{3} \in \mathbb{Q}$, such that $3 \cdot \frac{1}{3} = 1$. Thus, $\mathbb{Q}$ has a more robust algebraic structure than $\mathbb{Z}$ and makes it one of the most important subsets of real numbers. These algebraic properties that we articulate below, along with some technical ones, give the rationals $\mathbb{Q}$ the structure of a *field*.

- *Closed under Addition:* If $\dfrac{p_1}{q_1}, \dfrac{p_2}{q_2} \in \mathbb{Q}$, then their sum $\dfrac{p_1}{q_1} + \dfrac{p_2}{q_2} \in \mathbb{Q}$. To see this, notice that addition is given by

  $$\frac{p_1}{q_1} + \frac{p_2}{q_2} = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2},$$

  which is a rational number since its numerator and denominator are integers with its denominator non-zero.

- *Closed under Additive Inverses:* If $\dfrac{p}{q} \in \mathbb{Q}$, then there exists another rationals (namely $\dfrac{-p}{q} \in \mathbb{Q}$) such that

  $$\frac{p}{q} + \frac{-p}{q} = 0.$$

- *Closed under Multiplication:* If $\dfrac{p_1}{q_1}, \dfrac{p_2}{q_2} \in \mathbb{Q}$, then their product $\dfrac{p_1}{q_1} \cdot \dfrac{p_2}{q_2} \in \mathbb{Q}$. To see this, notice that multiplication is given by

  $$\frac{p_1}{q_1} \cdot \frac{p_2}{q_2} = \frac{p_1 p_2}{q_1 q_2},$$

  which is a rational number since its numerator and denominator are integers with its denominator non-zero.

- *Closed under Multiplicative Inverses:* If $\dfrac{p}{q} \in \mathbb{Q}$ is a non-zero rational number, then there exists another rational number (namely $\dfrac{q}{p} \in \mathbb{Q}$) such that

  $$\frac{p}{q} \cdot \frac{q}{p} = 1.$$

> Notice that $\dfrac{q}{p}$ is indeed a rational number since its numerator and denominator are integers and its denominator p is non-zero (since the original rational number was non-zero).

If we consider the rationals $\mathbb{Q}$ as a subset of the real numbers $\mathbb{R}$ and imagine where on the real line the set of rationals sits, it seems that they permeate almost all of $\mathbb{R}$. Towards this perspective, we show below that between any two distinct rational numbers, there exists another rational number.

Proposition. Let $a, b \in \mathbb{Q}$ be distinct rational numbers with $a < b$. There exists another rational number $x \in \mathbb{Q}$ such that

$$a < x < b.$$

Discussion.

`What we want:` To show that there exists an $x \in \mathbb{Q}$ with the property that

$$a < x < b.$$

`What we know:` $a, b \in \mathbb{Q}$ are *distinct* rational numbers and $a < b$. Thus, since $\mathbb{Q}$ is a field, we can add, subtract, multiply, or divide and obtain another rational number (if we divide, it cannot be by zero).

`What we'll do:` Since this is an existence proof, we will need to give the actual x that has the property $a < x < b$. If a and b are rationals, then taking the *average* of the two numbers will yield another rational (since $\mathbb{Q}$ is closed under addition and multiplication). Thus, we will let

$$x = \frac{a+b}{2}.$$

We must, of course, prove that x is indeed rational. We must further show that the desired inequality $a < x < b$ holds by showing that $a < x$ and that $x < b$.

Proof. Given two distinct rationals $a, b \in \mathbb{Q}$, let

$$x = \frac{a+b}{2}.$$

Notice that, since $a, b \in \mathbb{Q}$, then $a + b \in \mathbb{Q}$ since the rationals are closed under addition. Furthermore, $x = (a + b) \cdot \dfrac{1}{2}$, and since $a + b, \frac{1}{2} \in \mathbb{Q}$, x is also rational since $\mathbb{Q}$ is closed under multiplication.

Next, we show that $a < x < b$. Since $a < b$, we can add a to both sides to obtain $a + a < a + b$, which is equivalent to $2a < a + b$. Thus,

$$a = \frac{2a}{2} < \frac{a+b}{2} = x.$$

Similarly, since $a < b$, we can add b to both sides to obtain $a + b < b + b$, which is equivalent to $a + b < 2b$. Thus,

$$x = \frac{a+b}{2} < \frac{2b}{2} = b.$$

Thus, $a < x$ and $x < b$, giving us $a < x < b$, as desired.

Thus, $x = \dfrac{a+b}{2}$ is a rational number such that $a < x < b$.

□

Notice that, if $a < b$ are rationals, then the above propositions guarantees the existence of a rational x such that $a < x < b$. If we apply the proposition again to the two rationals $a < x$, then we obtain another rational y such that $a < y < x < b$. Continuing this process, we can building *infinitely many* rationals between any two distinct rationals. Intuitively, this means that the rationals are present in essentially all portions of the real line.

4.2.2 Irrational Numbers

Also important in the study of rational numbers are those real numbers that are not rational, called the *irrational numbers*. While there is no established convention for the set of irrational numbers, the notation

$$\mathbb{R} - \mathbb{Q}$$

is utilized fairly frequently.

In beginning the study of irrational numbers, it is not clear that an irrational even exists. We have heard multiple times in high school that important numbers like $\sqrt{2}, \pi$, and e are irrational, but most students were not offered proofs. Below, we will give a proof that $\sqrt{2}$ is an irrational number. Key to this proof is the fact that any rational number can be written in *lowest terms*. In other words, if $\dfrac{p}{q} \in \mathbb{Q}$ is rational, then, we can choose p and q to have no common divisors.

Since the set of irrational numbers are defined in terms of a negative statement (they are *not* rational), many statements involving rational numbers are easily proven using *proof by contradiction*, which we utilized in the Set Theory chapter when we proved a statement about complements of sets.

Recall that, in a proof by contradiction, if we wish to prove a statement p, then we assume its negation $\neg p$. With this assumption, we then proceed logically and arrive at a statement that contradicts some other established mathematical fact. Since this cannot logically occur, our initial assumption $\neg p$ must be false and thus p is true. Here, our p will be the statement that "$\sqrt{2}$ is an irrational number". Thus, its negation $\neg p$ is given by "$\sqrt{2}$ is a rational number" and thus we can use known facts about rationals to arrive at a contradiction.

Theorem. $\sqrt{2}$ is an irrational number.

Discussion.

`What we want:` We wish to show that $\sqrt{2}$ is an irrational number. Thus, we will use a proof by contradiction and assume that $\sqrt{2}$ is rational.

`What we'll do:` Since we are assuming $\sqrt{2}$ is a rational number, then we can write $\sqrt{2}$ as a fraction $\frac{p}{q}$, which is written in *lowest terms*. We will eventually contradict the fact that $\frac{p}{q}$ is in lowest terms by showing that they share a common divisor of two (since they will both be even). In doing so, we will use the previously proven theorem that "n^2 is even if and only if n is even."

Proof. Assume, to the contrary, that $\sqrt{2}$ is rational. Thus, we may write

$$\sqrt{2} = \frac{p}{q},$$

where p and q have no common divisors. Squaring both sides, we obtain

$$2 = \frac{p^2}{q^2},$$

which is equivalent to $2q^2 = p^2$. Notice that p^2 is even since it is written as a product of 2 and the integer q^2. Since $p^2 = p \cdot p$ is even, then p is even. Thus, we can write $p = 2r$ for some $r \in \mathbb{Z}$. Substituting, we get $2q^2 = p^2 = (2r)^2 = 4r^2$, which is equivalent to $q^2 = 2r^2$. Thus, q^2 is even, as it is the product of 2 and the integer q^2. As above, since $q^2 = q \cdot q$ is even, then q is even.

Thus, we have shown that both p and q are even, and so both p and q have a common divisor of 2, contradicting the assumption that p and q have no common divisors.

So, our initial assumption that $\sqrt{2}$ is rational must be false, and we conclude that $\sqrt{2}$ is irrational, as desired.

□

Above we have proven that $\sqrt{2}$ is an irrational number and thus non-rational real numbers exist. In the same way, one can prove that any $\sqrt{p}$ is an irrational number for any prime number p. In fact, arguing a little further, one can show that $\sqrt{m}$ is rational if and only if m is a perfect square. The proof that e and π are irrational are a bit more complicated and out of the scope of these notes.

We notice that, as important as the set of irrationals are, they do not enjoy the same algebraic properties as $\mathbb{Q}$. One major algebraic deficiency is the simple fact that 0 and 1, the *additive and multiplicative identities*, are not irrational. Furthermore, the irrationals are also deficient in the following ways.

- *Irrationals are Not Closed under Addition:* For example, $\sqrt{2}$ is irrational, and so is $-\sqrt{2}$ (we will show this later). However, $\sqrt{2} + -\sqrt{2} = 0$, which is not irrational.

- *Irrationals are Not Closed under Multiplication:* For example, $\sqrt{2}$ is irrational, but $\sqrt{2} \cdot \sqrt{2} = 2$ is not irrational.

Even though irrationals lack many nice algebraic properties, we can say something about the structure of this set. Below we give an example of such a proof. Again, since we are dealing with irrationals, *proof by contradiction* is an excellent option.

Propsoition. Let a be an irrational number. Then, $-a$ is irrational and $\frac{1}{a}$ is irrational.

Discussion. This proposition actually has two statements: $-a$ is irrational and $\frac{1}{a}$ is irrational. Since we wish to conclude two negative statements, it is natural to use proof by contradiction on both.

`What we know:` a is irrational. Thus, if we ever show that we can write a as a rational number, we know that we have arrived at a contradiction.

`What we want:`

- $-a$ is irrational. Thus, we will assume that $-a$ is rational and arrive a contradiction.

- $\frac{1}{a}$ is irrational. Thus, we will assume that $\frac{1}{a}$ is rational and arrive at a contradiction.

`What we'll do:`

- Since we assumed that $-a$ is rational, we will write is as $\frac{p_1}{q_1}$ and contradict the fact that a is irrational.

- Since we assumed that $\dfrac{1}{a}$ is rational, we can write it as $\frac{p_2}{q_2}$ and contradict the fact that a is irrational.

Proof. First, we will prove that $-a$ is irrational. Assume, to the contrary, that $-a$ is rational. Thus,

$$-a = \frac{p_1}{q_1},$$

where $p_1, q_1 \in \mathbb{Z}$ with $q \neq 0$. Multiplying by -1, we have

$$a = -(-a) = -\frac{p_1}{q_1} = \frac{-p_1}{q_1},$$

and we have thus written a as a fraction of two whole numbers with the denominator $q_1 \neq 0$. Thus, a is rational, a contradiction. Thus, our initial assumption that $-a$ is rational is false and thus $-a$ is irrational.

Next, we will prove that $\frac{1}{a}$ is irrational. First, notice that since a is irrational, then $a \neq 0$ because 0 is rational. Thus, $\frac{1}{a}$ is indeed a real number and not equal to 0. Assume, to the contrary, that $\frac{1}{a}$ is rational. Thus,

$$\frac{1}{a} = \frac{p_2}{q_2},$$

where $p_2, q_2 \in \mathbb{Z}$, $q_2 \neq 0$, and further $p_2 \neq 0$ since $\frac{1}{a} \neq 0$. Notice that

$$a = \frac{1}{1/a} = \frac{1}{p_2/q_2} = \frac{q_2}{p_2}.$$

Thus, we have written a as a fraction of two integers with its denominator p_2 being non-zero; thus, a is rational, a contradiction. So, our initial assumption that $\frac{1}{a}$ is rational is false and thus $\frac{1}{a}$ is irrational.

$\square$

Proposition. Let $a \in \mathbb{Q}$ be a non-zero rational and b be an irrational number. Then $a \cdot b$ is irrational.

Discussion.

`What we know:` a is a non-zero rational number and b is an irrational number. Since a is rational, we can use the nice field properties of $\mathbb{Q}$ when we are dealing with a.

`What we want:` $a \cdot b$ is irrational. Since this is a negative statement, we will use proof by contradiction. Thus, we will assume that $a \cdot b$ is rational and arrive at a contradiction.

`What we'll do:` We know that $0 \neq a \in \mathbb{Q}$ and thus a multiplicative inverse $\frac{1}{a}$ exists and is rational. Since we assumed that $a \cdot b$ is rational, then $b = \frac{1}{a} \cdot (a \cdot b)$ is a product of rationals and thus rational, a contradiction.

Proof. Assume, to the contrary, that $a \cdot b$ is rational. Since a is rational and non-zero, its multiplicative inverse $\frac{1}{a}$ exists and is a rational number. Since $\frac{1}{a}$ and $a \cdot b$ are rational numbers, their product is also rational. Thus,

$$\frac{1}{a} \cdot (a \cdot b) = \frac{1}{a} \cdot a \cdot b = b$$

is rational, contradicting the irrationality of b. So, our initial assumption that $a \cdot b$ is rational is false and thus $a \cdot b$ is irrational, as desired.

$\square$

Notice that, in fact, this most recent proposition is actually a generalization of the previous proposition stating that "if a is irrational, then $-a$ is irrational."