

1 The Real Numbers

In this course, we will primarily be studying properties of the real numbers. (In fact, we'll study a generalization called "metric spaces", which we'll define soon. But we can't talk about metric spaces without first understanding the real numbers well).

The real numbers are defined entirely by the fact that they are a "complete ordered field". They are in fact only complete ordered field that exists. But that probably doesn't tell you very much right now, because you probably don't know what any of those three things mean. So our first goal is to understand those three terms, and thus effectively define the real numbers.

1.1 Fields

First we need to define what a field is. The basic idea is that a field is a set where you can do addition, subtraction, multiplication, and division. More formally:

Definition 1.1. Suppose F is a set with two binary operations, $+$ and \times . We say F is a *field* if it satisfies the following axioms:

1. (Closure) If $x, y \in F$ then $x + y, xy \in F$.
2. (Commutativity) $x + y = y + x$ and $xy = yx$ for all $x, y \in F$.
3. (Associativity) $(x + y) + z = x + (y + z)$ and $(xy)z = x(yz)$ for all $x, y, z \in F$.
4. (Identities) There is an element $0 \in F$ such that $x + 0 = x$ for all $x \in F$. There is an element $1 \in F$ such that $1x = x$ for all $x \in F$.
5. (Inverses) For every $x \in F$ there is a $-x \in F$ such that $x + (-x) = 0$. For every non-zero $x \in F$ there is an element $x^{-1} \in F$ such that $xx^{-1} = 1$.
6. (Distributivity) $x(y + z) = xy + xz$ for all $x, y, z \in F$.

Example 1.2. The set \mathbb{Q} of rational numbers is a field. The sets \mathbb{R} and \mathbb{C} of real and complex numbers are fields.

The set \mathbb{Z} of integers is not a field, because it does not have multiplicative inverses. (We call this set a *ring*).

The set \mathbb{N} of natural numbers is not a field. It does not have multiplicative or additive inverses.

The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n is a field if n is prime, and is not a field if n is composite. (It is a fact we won't discuss again in this course that every number has a multiplicative inverse modulo n if and only if n is prime).

Proposition 1.3. *If $a, b \in F$ then there is a unique solution to the equation $x + a = b$. That is, there exists a unique $x \in F$ such that $x + a = b$.*

Proof. First we prove uniqueness. That is, we will suppose that x is a solution, and prove that there is only one possible value of x .

By inverses, we know that $-a$ exists. Since $x + a = b$ we have $(x + a) + (-a) = b + (-a)$.

By associativity, $(x + a) + (-a) = x + (a + (-a))$, and by inverses, $a + (-a) = 0$ so $x + (a + (-a)) = x + 0 = x$ by identity. Thus we have $x = b + (-a)$. So the only possible solution is $x = b + (-a)$.

Now we prove existence—which in this case, means proving that $b + (-a)$ is a solution. But we have

$$\begin{aligned}
 (b + (-a)) + a &= b + (-a + a) && \text{Associativity} \\
 &= b + (a + (-a)) && \text{Commutativity} \\
 &= b + 0 && \text{Inverses} \\
 &= b && \text{Identity}
 \end{aligned}$$

and thus $b + (-a)$ is a solution. □

Proposition 1.4. *Let F be a field and let $x_1, \dots, x_n \in F$. The meaning of the expression $x_1 + x_2 + \dots + x_n$ does not depend on the location of the parentheses, and thus we may omit parentheses without ambiguity.*

Proof. We prove this by induction. For a base case, suppose $n = 3$. Then by associativity, we know that $(x_1 + x_2) + x_3 = x_1 + (x_2 + x_3)$, and these are the only possible uses of parentheses, so the claim is true.

Now suppose the claim is true for a sum of n or fewer terms. Then we can rewrite any such sum to have the parentheses all on the left, as $((x_1 + x_2) + x_3) + \dots + x_n$. Now consider the sum $x_1 + \dots + x_{n+1}$. Any parenthesization will split it up as $(x_1 + \dots + x_k) + (x_{k+1} + \dots + x_{n+1})$ for some k .

By our inductive hypothesis, since the right-hand term has fewer than n terms, we can reparenthesize it with all the parentheses on the left to get $(x_1 + \dots + x_k) + (((x_{k+1} + \dots) +$

$x_n) + x_{n+1}$). By associativity, this is the same as $((x_1 + \cdots + x_k) + ((x_{k+1} + \cdots)) + x_n) + x_{n+1}$, and now the left-hand term has n terms, so by our inductive hypothesis we can put all the parentheses on the left, to get $((x_1 + x_2) + \cdots) + x_n + x_{n+1}$.

Thus every sum of n_1 terms, however parenthesized, can be rewritten with all parentheses to the left without changing the value. This proves our original claim that the value does not depend on the location of the parentheses. \square

Exercise 1.5. Prove that if F is a field and $x \in F$, then $0x = 0$.

1.2 Ordered Fields

We see that \mathbb{R} is one of many fields, so we need to be more specific in our description of it. One of the most important features of the real numbers is the real number line—which is just a way of saying we can put all the real numbers in order.

Definition 1.6. An *ordered set* is a set S with a total binary transitive anti-symmetric relation \leq . That is:

1. (Trichotomy) For any x, y in S , exactly one of the following is true: $x < y$ or $x = y$ or $y < x$; and
2. (Transitivity) If $x < y$ and $y < z$ then $x < z$.

We write $x \leq y$ if either $x < y$ or $x = y$. We define \geq and \geq in the obvious way: $x > y$ if and only if $y < x$.

It's possible to put an order on many sets just by arbitrarily deciding which things are smaller than which other things. (It's reasonable to say $\text{Red} < \text{Orange} < \text{Yellow} < \text{Green} < \text{Blue} < \text{Violet}$, for instance). The interesting question is whether you can order a set in a way compatible with its other properties.

Definition 1.7. A field F is an *ordered field* if it is an ordered set such that

1. (Order Additivity) If $x, y, z \in F$ and $x < y$ then $x + z < y + z$.
2. (Order Multiplicativity) If $x, y \in F$ with $x > 0, y > 0$, then $xy > 0$.

Remark 1.8. Rosenlicht gives an equivalent but distinct characterization, where he separates \mathbb{R} into the disjoint sets $\mathbb{R}_+, \{0\}, \mathbb{R}_-$, and asserts that \mathbb{R}_+ is closed under addition and multiplication; he then defines $x > y$ to mean that $x - y \in \mathbb{R}_+$.

This is sufficient to imply that \mathbb{R} is an ordered field under our definition; in fact, the properties we have stated are O1 through O4 in Rosenlicht. Rosenlicht's characterization has some benefits for the purpose of universal axiomatic constructions, but I think is a bit less clear about what's actually going on. My presentation thus follows Lebl instead.

We only stated a couple of principles here, but they imply a lot more. Most of the things they imply are things you're already taking for granted, but it's worth spelling them out—both because we need to know them, and because proving them is good practice for the sort of arguments we'll be making for the rest of the course.

Proposition 1.9. 1. $x > 0$ if and only if $-x < 0$.

2. If $x > 0$ and $y < z$ then $xy < xz$.

3. If $x < 0$ and $y < z$ then $xy > xz$.

4. If $x \neq 0$ then $x^2 > 0$.

5. $1 > 0$ in any field.

6. If $0 < x < y$ then $0 < y^{-1} < x^{-1}$.

7. If $0 < x < y$ then $x^2 < y^2$.

8. If $x \leq y$ and $z \leq w$ then $x + z \leq y + w$.

Proof. 1. $x > 0$, so by order additivity $x + (-x) > 0 + (-x)$, and thus $0 > -x$.

2. If $y < z$ then $y + (-y) < z + (-y)$ by order additivity, so $0 < z - y$. Then since $x > 0$, order multiplicativity gives us $0 < x(z - y)$, and distributivity gives $0 < xz - xy$. Finally, order additivity gives us $0 + xy < xz - xy + xy$, and thus $xy < xz$.

3. Exercise

4. If $x > 0$ then by order positivity, $x \cdot x > 0$.

If $x < 0$ then by the previous result, we have $x \cdot x > 0 \cdot 0 - 0$.

5. $1 = 1^2$, and $1^2 > 0$ by the previous result.

6. We know by field axioms that $\frac{1}{x} \neq 0$, $\frac{1}{y} \neq 0$. We first want to prove that both of them are positive. Suppose $\frac{1}{x} < 0$. Then $-\frac{1}{x} > 0$, and since $x > 0$, by order multiplicativity we have $-\frac{1}{x} \cdot x > 0$. Thus $-1 > 0$, which is a contradiction.

A similar argument shows that $\frac{1}{y} > 0$. So now we just need to show that $\frac{1}{y} > \frac{1}{x}$. But we know that $\frac{1}{x} \frac{1}{y} > 0$ by order multiplicativity; and since $x < y$, order multiplicativity tells us that $\frac{1}{x} \frac{1}{y} x < \frac{1}{x} \frac{1}{y} y$. Then multiplicative identities tells us that $\frac{1}{y} < \frac{1}{x}$.

7. Exercise

8. Exercise

□

Proposition 1.10. *Let $x, y \in F$ where F is an ordered field. Then $xy > 0$ if and only if either $x, y > 0$ or $x, y < 0$. $xy < 0$ if and only if either $x < 0, y > 0$ or $x > 0, y < 0$.*

Proof. If either $x = 0$ or $y = 0$, then $xy = 0$. So let's assume both x and y are nonzero.

If $x, y > 0$ then $xy > 0$ by definition of ordered field. If $x, y < 0$ then by proposition 1.9 we have $xy > x0 = 0$.

Now suppose x and y have opposite signs. Without loss of generality, assume $x > 0, y < 0$. Then by proposition 1.9 we have $xy < x0 = 0$. □

Example 1.11. \mathbb{R} is an ordered field, as is \mathbb{Q} .

The set $\mathbb{Z}/p\mathbb{Z}$ of integers modulo p is a field, but cannot be made into an ordered field. For suppose it were an ordered field. We will see that any square in an ordered field must be positive; since $1 = 1 \cdot 1$, we know that $1 > 0$. Then by positive additivity, we have $2 = 1 + 1 > 0 + 0 = 0, 3 = 1 + 1 + 1 > 0 + 0 + 0 = 0, \dots$. Adding p copies of 1 gives us 0, and thus we have $0 > 0$, which is a violation of the trichotomy principle.

Exercise 1.12. *Prove that \mathbb{C} cannot be an ordered field. (Hint: is $i > 0$, $i = 0$, or $i < 0$?)*

Definition 1.13. The *absolute value function* is defined by the formula

$$|a| = \begin{cases} a & a > 0 \\ 0 & a = 0 \\ -a & a < 0 \end{cases}$$

Proposition 1.14. 1. $|a| \geq 0$ for all $a \in \mathbb{R}$, and $|a| = 0$ if and only if $a = 0$.

2. $|ab| = |a| \cdot |b|$ for all $a, b \in \mathbb{R}$.

3. $|a|^2 = a^2$ for all $a \in \mathbb{R}$.

Lemma 1.15 (Triangle Inequalities). *Let $a, b \in \mathbb{R}$. Then*

1. $|a + b| \leq |a| + |b|$
2. $|a - b| \geq ||a| - |b||$.

Proof. 1. We know that $\pm a \leq |a|$ and $\pm b \leq |b|$. Thus $a + b \leq |a| + |b|$, and $-(a + b) \leq |a| + |b|$, by order additivity. Thus $|a + b| \leq |a| + |b|$.

2. This is really just the triangle inequality rearranged. In particular, we notice that $|a| = |a - b + b| \leq |a - b| + |b|$ by the triangle inequality. Adding $-|b|$ to both sides gives $|a| - |b| \leq |a - b| + |b| + (-|b|)$ by order additivity, and inverses and identity give us $|a| - |b| \leq |a - b|$.

We can make the same argument with a and b switched, which gives us $|b| - |a| \leq |b - a| = |a - b|$. Thus these two statements together give us $||a| - |b|| \leq |a - b|$.

□

We sometimes want to turn expressions involving absolute value into expressions that don't. The following proposition is useful for this:

Proposition 1.16. $|x - a| < \epsilon$ if and only if $a - \epsilon < x < a + \epsilon$.

Proof. $|x - a| < \epsilon$ if and only if $x - a < \epsilon$ and $a - x < \epsilon$. The first inequality is equivalent to $x < a + \epsilon$ by order addition; the second is equivalent to $a - \epsilon < x$. □

1.3 The Least Upper Bound Property

We now understand what an ordered field is, but we've identified at least two: \mathbb{Q} and \mathbb{R} . (In fact there are infinitely many ordered fields that contain \mathbb{Q} and are contained in \mathbb{R} ; an example is $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$).

If we want to understand what makes \mathbb{R} special, we need one extra property. Formally this property is called “completeness”, a term which we will return to later in the course. Here we can give a much simpler characterization.

Definition 1.17. Suppose F is an ordered field, and $S \subset F$. We say that a is an *upper bound* for S if $s \leq a$ for all $s \in S$. If S has an upper bound, we say that it is *bounded above*.

We say that y is a *least upper bound* of S if y is an upper bound for S , and if a is also an upper bound for S , then $y \leq a$. We sometimes write that $y = \sup S$.

Lemma 1.18. *Let F be an ordered field and $S \subset F$. If S has an least upper bound, then that upper bound is unique.*

Proof. Suppose that a and b are both least upper bounds of S . Then since a is a least upper bound and b is an upper bound, then by definition of least upper bound $a \leq b$.

But b is a least upper bound and a is an upper bound, so by definition of least upper bound $b \leq a$.

Since $a \leq b$ and $b \leq a$, we know that $a = b$. □

Exercise 1.19. Let F be an ordered field and $S \subset F$. Let y be a least upper bound of S , and let $x < y$. Prove that there is an $s \in S$ such that $x < s$.

Example 1.20. Let $S = \{x : x \leq 0\}$ be a subset of \mathbb{R} . Then we claim that 0 is the least upper bound for S .

First we prove that 0 is an upper bound for S . If $x \in S$ then $x \leq 0$ by definition of S .

Now we prove that 0 is a least upper bound—that is, we prove that if y is an upper bound for S , then $0 \leq y$. But suppose that y is an upper bound for S . Then since $0 \in S$, we have that $0 \leq y$. Thus 0 is the least upper bound for S .

Example 1.21. Let $S = \{x : x < 0\}$ be a subset of \mathbb{R} . Then we claim that 0 is a least upper bound for S .

If $x \in S$ then $x < 0$, so $x \leq 0$, so 0 is an upper bound for S .

Now we want to prove that 0 is the least upper bound. We can't do the same thing we did last time, because 0 is not an element of S . Instead we do a proof by contradiction.

Let y be an upper bound for S , and suppose $y < 0$. By properties of ordered fields, since $1 > \frac{1}{2}$ we know that $y < y/2$, and since $\frac{1}{2} > 0$ we know that $y/2 < 0$. Thus $y/2 \in S$ and $y < y/2$, contradicting our assumption that y was an upper bound for S .

Thus if y is an upper bound for S , we have $y \geq 0$, so 0 is the least upper bound.

Example 1.22. Let $S = \{x : x^2 < 2\}$ be a subset of \mathbb{Q} . Then S is bounded above, for instance, $x < 2$ for all $x \in S$. But S has no least upper bound in \mathbb{Q} .

Definition 1.23. Let F be an ordered field and let S be a subset of F . We say that S has the *Least Upper Bound Property* if, whenever T is a non-empty subset of S and T is bounded above, then T has a least upper bound in S .

Now we can completely characterize the real numbers: \mathbb{R} is the unique ordered field that satisfied the Least Upper Bound property. Whenever we have a set of real numbers that is bounded above, there is a real number that is the least upper bound for that set.

Lemma 1.24 (Archimedean Property). *If $x \in \mathbb{R}$, then there exists a $n \in \mathbb{N}$ such that $n > x$.*

Proof. Suppose this is false; then there is some real number x such that $n \leq x$ for all $n \in \mathbb{N}$. This would mean that \mathbb{N} is bounded above, and by the Least Upper Bound property it must have a least upper bound a .

But if n is a natural number, then so is $n + 1$, so we see that $n + 1 \leq a$ for all $n \in \mathbb{N}$. Then $n \leq a - 1$ for all $n \in \mathbb{N}$, which means that $a - 1$ is an upper bound for \mathbb{N} ; but $a - 1 < a$, contradicting the assumption that a is a least upper bound.

Thus no least upper bound can exist; so the set of integers cannot be bounded above by x . This proves our lemma. \square

Exercise 1.25. Prove that for any real number $\epsilon > 0$, there is a $n \in \mathbb{N}$ such that $1/n < \epsilon$.

Proposition 1.26. For any $x \in \mathbb{R}$, there is an integer $n \in \mathbb{Z}$ such that $n \leq x < n + 1$.

Proof. By the Archimedean property, there is an N such that $N > |x|$. Consider the set of integers $S = \{n : -N < n < N\}$. This is a finite set, so we can take the largest n in S such that $n \leq x$.

Then we claim $n + 1 > x$. Otherwise, we would have $n + 1 < N$, so it would be in S , and n wouldn't be the largest element of S that is less than or equal to x . \square

Corollary 1.27. For any $x \in \mathbb{R}$ and any positive integer N , there is an integer n such that $\frac{n}{N} \leq x < \frac{n+1}{N}$.

Proposition 1.28. For every $x \in \mathbb{R}$ and $\epsilon > 0$, there is a rational number $r \in \mathbb{Q}$ such that $|x - r| < \epsilon$.

Proof. By our exercise 1.25, we know there is a positive integer N with $1/N < \epsilon$. Then by corollary 1.27 there is some integer n with $n/N \leq x < (n + 1)/N$, so we have $0 < x - \frac{n}{N} < \frac{n+1}{N} - \frac{n}{N} = \frac{1}{N}$.

Since these numbers are all positive, we can take absolute values, and we get $0 < |x - \frac{n}{N}| < \frac{1}{N}$. Thus we take our rational number $r = \frac{n}{N}$. \square

1.4 Constructing the Real Numbers

So what do the real numbers look like? We know the real numbers contain all the rational numbers; this gives us an ordered field. And the real numbers satisfy the Least Upper Bound property. So what extra numbers does this give us?

Proposition 1.29. Let x be a positive real number. Then there is a unique positive real number y such that $y^2 = x$.

Proof. If $0 < y_1 < y_2$ then $y_1^2 < y_2^2$, so any positive square root is unique. We just need to show that a positive square root exists.

Let $S = \{a \in \mathbb{R} : 0 \leq a^2 < x\}$. Then S is non-empty, since $0 \in S$, and S is bounded above by $\max\{1, x\}$, since $a < a^2$ for $a \geq 1$. By the Least Upper Bound principle, we know that S has a least upper bound; let $y = \sup(S)$. We claim that $y^2 = x$.

First we observe that $y > 0$. We know that $(\min\{1, x\})^2 \leq \min\{1, x\} \cdot 1 = \min\{1, x\} < x$, so $\min\{1, x\} \in S$; and since $1, x > 0$ we know that $\min\{1, x\} > 0$. Thus $y \geq \min\{1, x\} > 0$.

Now for any real number ϵ with $0 < \epsilon < y$, we see that $0 < y - \epsilon < y < y + \epsilon$, and so $(y - \epsilon)^2 < y^2 < (y + \epsilon)^2$. But we can also see that since $y - \epsilon \in S$, then $(y - \epsilon)^2 < x$, and since $y + \epsilon \notin S$ we know that $(y + \epsilon)^2 \geq x$. We conclude that $(y - \epsilon)^2 < x < (y + \epsilon)^2$. Then order additivity gives us

$$\begin{aligned} (y - \epsilon)^2 &< y^2 < (y + \epsilon)^2 \\ (y - \epsilon)^2 &< x < (y + \epsilon)^2 \\ (y - \epsilon)^2 - (y + \epsilon)^2 &< y^2 - x < (y + \epsilon)^2 - (y - \epsilon)^2 \\ |y^2 - x| &< (y + \epsilon)^2 - (y - \epsilon)^2 = 4y\epsilon. \end{aligned}$$

But this inequality holds for any ϵ with $0 < \epsilon < y$, so for any $a > 0$ we can choose ϵ so that $4y\epsilon < a$. Thus $|y^2 - x| < a$ for all $a > 0$, and so $|y^2 - x| = 0$. Thus $y^2 = x$ as claimed. \square

As a corollary, this tells us that there are real numbers which are not rational numbers: $\sqrt{2}$ is a real number, but is not rational.

It also tells us that the order of the reals is more or less uniquely specified. We just saw that the set of positive real numbers is precisely the set of squares of real numbers. That is, $\{x : x \geq 0\} = \{y^2 : y \in \mathbb{R}\}$. Since knowing the set of positive real numbers is enough to determine the order completely, this means that the Least Upper Bound property allows only one possible order structure.

But how can we be sure we've found all the real numbers? Here we can turn to infinite decimals.

Definition 1.30. If a_0 is any integer, n a positive integer, and a_1, \dots, a_n are elements of the set $\{0, \dots, 9\}$, then we define the finite decimal

$$a_0.a_1 \dots a_n = a_0 + \frac{a_1}{10} + \dots + \frac{a_n}{10^n}.$$

Remark 1.31. If $a_0 < 0$ this is actually not the usual way we interpret a finite decimal; but it's much more convenient for what we're doing. The difference doesn't matter to anything terribly important.

If $m < n$, we see that

$$\begin{aligned} a_0.a_1 \dots a_m &\leq a_0.a_1 \dots a_m + a_{m+1}10^{-m-1} + \dots + a_n10^{-n} \\ &\leq a_0.a_1 \dots a_m + 9 \cdot 10^{-m-1} + \dots + 9 \cdot 10^{-n} \\ &< a_0.a_1 \dots a_m + 10^{-m} \end{aligned}$$

where we obtain the last inequality by adding 10^{-n} to the previous expression. This means that for any finite decimal, we have the bounds

$$a_0.a_1 \dots a_m \leq a_0.a_1 \dots a_n < a_0.a_1 \dots a_m + 10^{-m}.$$

This allows us to define infinite decimals:

Definition 1.32. If a_0 is any integer and a_1, a_2, \dots is a sequence of elements of $\{0, \dots, 9\}$, then we define the *infinite decimal* $a_0.a_1a_2\dots$ to be the least upper bound of the set $\{a_0.a_1 \dots a_n : n \in \mathbb{N}\}$.

For this definition to make sense, we need to check that this set *has* a least upper bound. But we know the set is bounded above, for example by $a_0 + 1$; thus by the Least Upper Bound principle it has a least upper bound in \mathbb{R} .

Proposition 1.33. *Every real number can be represented by an infinite decimal.*

Proof. Let $x \in \mathbb{R}$. Then by corollary 1.27, taking $N = 10^{-m}$, there is some finite decimal $a_0.a_1 \dots a_m$ such that

$$a_0.a_1 \dots a_m < x < a_0.a_1 \dots a_m + 10^{-m}.$$

We can do this for any m , and if $n > m$ then the first m terms of both finite decimals will be the same. Thus we can define an infinite decimal by taking these $a_0.a_1 \dots a_m$ for each $m \in \mathbb{N}$, and then x is equal to this infinite decimal. \square

Thus we've seen that every real number can be given by an infinite decimal. And this means that the entire field \mathbb{R} is uniquely specified. We've seen that there is only one order we can choose compatible with the Least Upper Bound principle; and given that order, the set of real numbers is precisely the set of infinite decimals. This justifies our definition that \mathbb{R} is "the" complete ordered field.

Remark 1.34. There are two other definitions or “constructions” of the reals you will sometimes see. Both of them construct sets of rational numbers, and define real numbers to be equivalence classes of these sets of rational numbers.

Later in this course we will see how we could define the reals to be equivalence classes of “Cauchy sequences” of rational numbers. This just means that a real number is the limit of some sequence of rational numbers—and if a sequence looks like it should converge, but there is no rational number it converges to, we call that a real number.

The most rigorous construction is via the use of Dedekind cuts. Here we define real numbers to be equivalence classes of partitions of the rational numbers into two sets, where the first is strictly smaller than the second and contains no greatest element. So the square root of two would be the partition (A, B) where $A = \{a \in \mathbb{Q} : a^2 < 2 \text{ or } a < 0\}$, and $B = \{b \in \mathbb{Q} : b^2 \geq 2 \text{ and } b \geq 0\}$.

We can then define addition and multiplication on these partitions, and check that they satisfy the field axioms, and the order axioms, and the least upper bound property. But this is tedious and not terribly enlightening, so we’ll avoid it.

If you want to learn more about this, you can see p.186 of Rogers and Boman, which is available free online and linked in the syllabus.