MATH 521, WEEK 3:
Supremum and Infimum, Fields

1 Maximum and Minimum

Consider a subset $S \subseteq X$ where X is some ordered set. For simplicity, we may think of X as either $\mathbb{Q}$ or $\mathbb{R}$; indeed, most of our examples will be drawn from these well-known sets. We identify the following elements of S.

Definition 1.1. *Suppose $S \subseteq X$ where X is an ordered set. We will say that $x \in S$ is the **maximum** of S (denoted $\max(S)$) if $x \geq y$ for all $y \in S$. Correspondingly, we will say that $x \in S$ is the **minimum** of S (denoted $\min(S)$) if $x \leq y$ for all $y \in S$.*

A key feature of minima and maxima which will distinguish them from further objects we will consider is that *they are contained in the set of interest*. It does not make sense say $x = \max(S)$ or $x = \min(S)$ if $x \notin S$. We start with a basic result.

Theorem 1.1. *Suppose $S \subseteq X$ where X is an ordered set. Then, if $\max(S)$ (or $\min(S)$) exists, it is unique.*

Proof. Suppose $S \subseteq X$ where X is an ordered set and there exist $x, y \in S$, $x \neq y$, so that $x = \max(S)$ and $y = \max(S)$. It follows that (1) $x \geq z$ for all $z \in S$, and (2) $y \geq z$ for all $z \in S$. Since $y \in S$, it follows from (1) that $x \geq y$, and since $x \in S$, it follows from (2) that $y \geq x$. It follows from $x \geq y$ that either $x > y$ or $x = y$ while it follows from $y \geq x$ that either $y > x$ or $y = x$. The only consistent combination of choices is $x = y$, which is a contradition, and the result is shown. □

In other words, we are justified in saying *the* maximum and *the* minimum of an ordered set. To see other subtleties which may arise, consider the following examples.

Example 1: Find the maximum and minimum of the set $S = \{3, -1, 2, 4\}$.

Solution: We quickly identify that $\min(S) = -1$ and $\max(S) = 4$ since $-1 \leq x \leq 4$ for all $x \in S$.

Example 2: Find the maximum and minimum of the set

$$S = \{y \in \mathbb{R} \mid y = 2x^2 - 4x + 7, x \in [0, 3]\}.$$

Solution: We recognize this as a standard problem from introductory calculus. Allowing that the maximum and minimum may only be obtained for continuous functions at critical points and endpoints of intervals (a detail for later in the course!), we quickly compute that, for $f(x) = y$, we have

$$f'(x) = 4x - 4 = 0 \quad \Longrightarrow \quad x = 1.$$

It follows from $f(0) = 7$, $f(1) = 5$, and $f(3) = 13$ that $\min(S) = 5$ and $\max(S) = 13$. Note that, as in the last example, we have $5 \leq y \leq 13$ for all $y \in S$.

Example 3: Find the maximum and minimum of the following sets:

$$A = \{2, 4, 6, 8, 10, \ldots\}$$
$$B = \left\{ \frac{1}{n} \mid n \in \mathbb{N} \right\}.$$

Solution: We immediately recognize the set A as corresponding to the set of positive *even* numbers. It is clear that, while we can identify the minimal element as $\min(A) = 2$, there is no maximal element. No matter how high an even number we have in our hands, however, we can always reach out and find a higher one. It follows that $\max(A)$ does not exist.

Now consider the set B. We can enumerate a few elements as follows:

$$B = \left\{ 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots, \right\}.$$

It is clear that $\max(B) = 1$ since $1/n > 1/(n+1)$ for all $n \in \mathbb{N}$, but $\min(B)$ is another story altogether. It is clear that the elements in the set get closer and closer to zero without exceeding it (i.e. for every $\epsilon > 0$, there is an $n \in \mathbb{N}$ such that $0 < 1/n < \epsilon$). However, we *cannot* conclude that zero is the minimum of the set because *zero is not in the set* B (i.e. $0 \notin B$). But for every $n \in \mathbb{N}$ there is an $m \in \mathbb{N}$ so that $1/n > 1/m$. In fact, there are *infinitely* many. It follows that the set does not have a minimal element, i.e. $\min(B)$ does not exist.

2 Supremum and Infimum

We have identified two ways in way a maximum or minimum may not exist: if the set is unbounded and if the set can be arranged into some sort of monotone limit but never reaches the limiting value.

This should be somewhat unsatisfying, especially the second case. After all, we can clearly identify that the set B is *bounded from below*. That is to say, we have that there is an $m \in \mathbb{R}$ so that $x \geq m$ for all $x \in B$. This is practically the definition of $\min(S)$, but, because $m \notin S$, $\min(S)$ is insufficient to capture the notion of having a lower bound. We are prevented from assigning $\min(S)$ by a technicality! (Notice that $\max(S)$ may be insufficient to describe how high a set can get, for the same reason.)

As a first stab at overcoming this insufficiency, we introduce the following concepts.

Definition 2.1. *Suppose $S \subseteq X$ where X is an ordered set. We will say that S is **bounded from above** if there exists an $M \in X$ so that $x \leq M$ for all $x \in S$, and call M an **upper bound** of S. We will say that S is **bounded from below** if there exists an $m \in X$ so that $x \geq m$ for all $x \in S$, and call m a **lower bound** of S.*

Definition 2.2. *Suppose $S \subseteq X$ where X is an ordered set. Then $\alpha \in X$ is said to be the **supremum** of S (respectively, **infimum** of S) if:*

1. *α is an upper bound of S (respectively, lower bound of S); and*
2. *If $\beta \in X$ is an upper bound of S such that $\beta \neq \alpha$, then $\alpha < \beta$ (respectively, if $\beta \in X$ is a lower bound of S such that $\beta \neq \alpha$, then $\beta < \alpha$).*

The supremum of S is denoted $\sup(S)$ *while the infimum is denoted* $\inf(S)$.

Note: Another way of stating the second condition (for supremums) is that, if $\beta < \alpha$, then β is not an upper bound of S. That is to say, for any $\beta \in X$ such that $\beta < \alpha$, there is an $x \in S$ so that $\beta < x < \alpha$. The condition for infimums is analogous.

To determine the supremum of S, we need to find an upper bound of S (point (1)) which is minimal among *all* upper bounds (point (2)). The key point which separates $\sup(S)$ and $\inf(S)$ from $\max(S)$ and $\min(S)$ is that we no longer require the bound to be in the set S itself.

Note: The supremum of S is also known as the **least upper bound** of S while the infimum of S is also known as the **greatest lower bound**. The reason should be clear from the definitions.

Example 3 (revisited): Determine $\sup(B)$ and $\inf(B)$ for

$$B = \left\{ \frac{1}{n} \mid n \in \mathbb{N} \right\}.$$

Solution: We can see that $\sup(B) = 1$ because $\max(B) = 1$ (since $1 \geq x$ for all $x \in B$). But now we also have a grasp on how to consider how small the set may get. We have that zero is a lower bound since $1/n > 0$ for all $n \in \mathbb{N}$. Furthermore, we can see that zero is the greatest possible lower bound since, for any $\epsilon > 0$, there is an $n \in \mathbb{N}$ such that $0 < 1/n < \epsilon$. It follows that any such $\epsilon > 0$ is not a lower bound, and therefore that $\inf(B) = 0$.

This is fantastic! We seem to have closed one the loopholes we have previous left open. If we cannot find a maximal or minimal element from the set S itself, we seem to be able to accomplish the same task by expanding our search to the larger set X. But is this really enough? Is it true, for instance, that if a set is bounded above in X that $\sup(S)$ always exists (in X)? Consider the following example.

Example 4: Determine $\sup(S)$ for

$$S = \left\{ x \in \mathbb{Q} \mid x^2 < 2 \right\}.$$

Solution: This problem looks very much like a problem we have already considered, namely, how the rational numbers are embedded in the real numbers. The moral we are trying to establish now, however, is subtly different.

Consider determining $\sup(S)$. It is clear that $\sqrt{2}$ is an upper bound of S (by the definition of S) and that $\sqrt{2} \notin S$. Furthermore, we have $\sqrt{2} \notin \mathbb{Q}$ so that, because $X = \mathbb{Q}$ for this example, we have $\sqrt{2} \notin X$. So we have an upper bound which is not in S *or* X!

To conclude, however, that $\sup(S)$ does not exist in $\mathbb{Q}$, however, we need to show that there is no least upper bound in $\mathbb{Q}$. Consider a rational number q so that $q < \sqrt{2}$. From an earlier result, we know that there is a rational number in between any two real numbers. It follows that there is a $p \in \mathbb{Q}$ such that $q < p < \sqrt{2}$. Since we clearly have $p \in S$, we have that q is not an upper bound of S.

Now consider searching for a least upper bound satisfying $\sqrt{2} < q$. While every such q is an upper bound of S, we may not select a *least* upper bound because there must be a rational number $p \in \mathbb{Q}$ so that $\sqrt{2} < p < q$. q is therefore not minimal. We are forced to conclude that the supremum does not exist within the ordered set $\mathbb{Q}$.

This should be slightly unsettling, but maybe not surprising. We already know the rational numbers are insufficient in many ways, since there are many (an *uncountable* many!) numbers which cannot be expressed as rational numbers. Nevertheless, we would definitely like to be able to define the notation of smallest and largest elements of a set. This seems like a basic thing, and yet the rational numbers cannot do it!

To overcome this difficulty, we define the following concept.

Definition 2.3 (Definition 1.10, Rudin)**.** *Suppose X is an ordered set. Then X is said to have the* ***least upper bound property*** *if, for every nonempty $S \subseteq X$ which is bounded above, we have that* $\sup(S) \in X$.

This is exactly the property we just discussed! We can clearly see that the rational numbers *do not have* the least upper bound property since $\sup(S) \notin \mathbb{Q}$ for the set S defined in Example 4. Let's prove some properties of sets with this property.

Theorem 2.1 (Theorem 1.11, Rudin)**.** *Suppose $S \subseteq X$ where X is an ordered set with the least upper bound property. Suppose S is nonempty and bounded from below. Then* $\inf(S) \in X$.

This result simply states that it is unnecessary to define and consider both a *least upper bound property* and an analogous *greatest lower bound property* for an ordered set X. One necessarily implies the other.

Proof. The proof is actually easier than it seems. We will consider the set of all lower bounds of S (because S is bounded below), and then use the show the *supremum* of this set exists in X (by the least upper bound property of X). It is then straight-forward to verify that this is the infimum of S.

First, define $L = \{\alpha \in X \mid \alpha \leq x, \text{ for all } x \in S\}$. We have that L is nonempty because S is bounded below. Since $L \subseteq X$ and L is bounded above (by S), it follows that $\sup(L) \in X$ by the least upper bound property of X. Let $\alpha = \sup(L)$.

We prove now that α is a lower bound of S (i.e. $\alpha \in L$). Suppose otherwise. That is to say, suppose there is an $x \in S$ such that $x < \alpha$. Since $x \in S$, however, we have that $y \leq x$ for all $y \in L$ so that x is an upper

bound of L. It follows that $\alpha \neq \sup(L)$, which is a contradition. It follows that $\alpha \in L$.

Now suppose $\alpha \neq \inf(S)$. Since we know α is a lower bound of S, it follows that there is a $\gamma \in X$ such that $\alpha < \gamma$ and $\gamma \leq y$ for all $y \in S$ (since there must be a greater lower bound). This implies that $\gamma \in L$. However, $\alpha < \gamma$ and $\gamma \in L$ implies that $\alpha \neq \sup(L)$, which is a contradiction. It follows that our assumption was invalid, so that it must be true that $\sup(L) = \inf(S) \in X$, and we are done. □

This raises the question of how exactly the rational numbers and real numbers are related by the order operator $<$. We have the following result.

Theorem 2.2 (Theorem 1.19, Rudin)**.** *The real numbers $\mathbb{R}$ have the least-upper-bound property. Furthermore, for every $S \subseteq \mathbb{Q}$ which is bounded above, there exists an $x \in \mathbb{R}$ such that $x = \sup(S)$.*

In other words, we do not have to go any further than the real numbers if we want to *complete* the rational numbers in terms of upper (and lower) bounds. Another way to state this is that the minimal superset of the rational numbers which has the least upper bound property is the real numbers. This is the way it is stated in Rudin.

Note: The proof for this result is beyond the scope of this course, but the interested reader is referred to the Appendix of Chapter 1 of Rudin. It is an interesting argument in that it actually *constructs* the real number system $\mathbb{R}$ from the rational numbers $\mathbb{Q}$. The formal argument takes particular subsets of $\mathbb{Q}$, called *Dedekind cuts*, and proves that these subsets form an ordered set with the least upper bound property.

We can finally prove a result we stated (and used) last week.

Theorem 2.3 (Archimedean Property)**.** *If $x, y \in \mathbb{R}$, and $x > 0$, then there is a natural number $n \in \mathbb{N}$ such that $nx > y$.*

Proof. Suppose otherwise, i.e. suppose there are $x, y \in \mathbb{R}$ with $x > 0$ for which there does not exist an $n \in \mathbb{N}$ so that $nx > y$. That is to say, for every $n \in \mathbb{N}$, we have $nx \leq y$. It follows that y is an upper bound for the set $S = \{nx \mid n \in \mathbb{N}\}$. Since $\mathbb{R}$ has the least upper bound property, we have that $\sup(S) \in \mathbb{R}$. Let $\alpha = \sup(S)$. Since $x > 0$, we have that $-x < 0$ so that $\alpha - x < \alpha$ so that $\alpha - x$ is not an upper bound of S. It follows that $\alpha - x < mx$ for some $m \in \mathbb{N}$. It follows directly from this expression, however, that $\alpha < mx + x = (m + 1)x \in S$ (since $(m + 1) \in \mathbb{N}$). It follows

that α is *not* and upper bound of S, which is a contradiction. It follows that our assumption was made in error, and we are done. $\square$

3 Fields

We have given a lot of consideration to the rational and real number systems. In particular, we have considered extensively how they relate to one another through the order operator $<$. We now know that the rational numbers are *dense* in the real numbers, and that the real numbers are the minimal superset of the rational numbers with the least upper bound property.

What we might feel is notably lacking so far is any discussion of *arithmetic*. After all, we have introduced nothing (at least formally) which tells us how we may *manipulate* elements of $\mathbb{Q}$ and $\mathbb{R}$ (although we have assumed traditional operations at several points). To be rigorous, we now introduce the following fundamental concept.

Definition 3.1 (Definition 1.12, Rudin)**.** *A set $\mathbb{F}$ is said to be a **field** if it has two operations "$+$" and "$\cdot$" (additional and multiplication, respectively) which satisfy the following:*

(A) ***Addition****:*

- *(A1) $x, y \in \mathbb{F}$ implies $x + y \in \mathbb{F}$ (Closure);*
- *(A2) $x + y = y + x$ for all $x, y \in \mathbb{F}$ (Commutativity);*
- *(A3) $(x + y) + z = x + (y + z)$ for all $x, y, z \in \mathbb{F}$ (Associativity);*
- *(A4) There exists an element $0 \in \mathbb{F}$ so that $x + 0 = x$ for all $x \in \mathbb{F}$ (Identity);*
- *(A5) For every $x \in \mathbb{F}$, there exists an element $-x \in \mathbb{F}$ so that $x + (-x) = 0$ (Inverse).*

(M) ***Multiplication****:*

- *(M1) $x, y \in \mathbb{F}$ implies $x \cdot y \in \mathbb{F}$ (Closure);*
- *(M2) $x \cdot y = y \cdot x$ for all $x, y \in \mathbb{F}$ (Communitativity);*
- *(M3) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in \mathbb{F}$ (Associativity);*
- *(M4) There exists an element $1 \in \mathbb{F}$ so that $x \cdot 1 = x$ for all $x \in \mathbb{F}$ (Identity);*
- *(M5) For every $x \in \mathbb{F}$ such that $x \neq 0$, there exists an element $x^{-1} \in \mathbb{F}$ so that $x \cdot x^{-1} = 1$ (Inverse).*

(D) ***Distributive law:*** *$x \cdot (y + z) = x \cdot y + x \cdot z$ for all $x, y, z \in \mathbb{F}$.*

It is easy to show that $\mathbb{Q}$ and $\mathbb{R}$ are fields since these axioms for arithmetic correspond to our conventional understanding of additional and multiplication. A surprising feature of the field axioms, however, is that many further arithmetic properties which we often take for granted with $\mathbb{Q}$ and $\mathbb{R}$ follow directly from the axioms themselves. Consider the following.

Theorem 3.1 (Roughly Proposition 1.14 & 1.15, Rudin)**.** *Suppose $\mathbb{F}$ is a field.*

1. *It follows by the axioms of addition (A1-5) that:*
   (a) *The additive identity element $0 \in \mathbb{F}$ is unique.*
   (b) *For each $x \in \mathbb{F}$, the additive inverse element $-x \in \mathbb{F}$ is unique.*
   (c) *For each $x \in \mathbb{F}$, $-(-x) = x$.*
2. *It furthermore follows by the axioms of multiplication (M1-5) that:*
   (a) *The multiplicative identity element $1 \in \mathbb{F}$ is unique.*
   (b) *For each $x \in \mathbb{F}$, $x \neq 0$, the multiplicative inverse element $x^{-1} \in \mathbb{F}$ is unique.*
   (c) *For each $x \in \mathbb{F}$, $x \neq 0$, we have $(x^{-1})^{-1} = x$.*

Proof. 1.(a): Suppose $x + y = x$ for $x, y \in \mathbb{F}$. We wish to show that $y = 0$. From the axioms, we have

$$\begin{aligned} y &= y + 0 && (A4) \\ &= y + (x + (-x)) && (A5) \\ &= (y + x) + (-x) && (A3) \\ &= (x + y) + (-x) && (A2) \\ &= x + (-x) && \text{(assumption)} \\ &= 0 && (A5). \end{aligned}$$

In other words, we have that the only element which can satisfy $x + y = x$ for any $x \in \mathbb{F}$ is $y = 0 \in \mathbb{F}$. It follows that the addictive identity is unique.

1.(b): Suppose $x + y = 0$ for $x, y \in \mathbb{F}$. We wish to show that $y = -x$. From the axioms, we have

$$\begin{aligned} y &= y + 0 && (A4) \\ &= y + (x + (-x)) && (A5) \\ &= (y + x) + (-x) && (A3) \\ &= (x + y) + (-x) && (A2) \\ &= 0 + (-x) && \text{(assumption)} \\ &= -x && (A4). \end{aligned}$$

So, for a given $x \in \mathbb{F}$, we have that $x + y = 0$ implies that $y = -x$. That is to say, for each $x \in \mathbb{R}$, the addictive inverse is unique.

1.(c): Consider $x \in \mathbb{F}$. We have that there is a unique $-x \in \mathbb{F}$ so that $x + (-x) = 0$. Since $-x \in \mathbb{F}$, we furthermore have $-(-x) \in \mathbb{F}$ and that $-x + (-(-x)) = 0$. It follows that

$$\begin{aligned} x &= x + 0 && (A4) \\ &= x + ((-x) + (-(-x))) && (A5) \\ &= (x + (-x)) + (-(-x)) && (A3) \\ &= 0 + (-(-x)) && (A2) \\ &= -(-x) && (A4). \end{aligned}$$

2.(a-c): Follows similarly! □

We might notice that we have not used the distributive law (D) for any those results. Before we begin to think it really is not used at all, we might realize that none of the results so far say anything about how the addition and multiplication operations *interact* with one another. This is where we will need the distributive law! We have the following result.

Theorem 3.2 (Proposition 1.16 in Rudin)**.** *Suppose $\mathbb{F}$ is a field. Then we have*

3.(a) $0 \cdot x = 0$ *for all* $x \in \mathbb{F}$.

3.(b) $0 \neq 1$.

3.(c) For any $x, y \in \mathbb{F}$, $x \cdot y \neq 0$ *if and only if* $x \neq 0$ *and* $y \neq 0$.

3.(d) $(-x) \cdot y = -(x \cdot y) = x \cdot (-y)$ *for all* $x, y \in \mathbb{F}$.

3.(e) $(-x)\cdot(-y) = x\cdot y$ *for all* $x, y \in \mathbb{F}$.

Proof. 3.(a): For any $x \in \mathbb{F}$, we have

$$\begin{aligned} 0\cdot x + 0\cdot x &= (0+0)\cdot x && (D) \\ &= 0\cdot x && (A4). \end{aligned}$$

It follows that $0\cdot x$ is the additive inverse, which we know is unique by $1.(a)$. It follows that $0\cdot x = 0$.

3.(b): For any $x \in \mathbb{F}$, from $3.(a)$ we have

$$x = 1\cdot x = 0\cdot x = 0.$$

This clearly does not hold for all $x \in \mathbb{F}$ so that we have a contradiction, and $1 \neq 0$.

3.(c): Clearly $x = 0$ or $y = 0$ implies $x\cdot y = 0$ by 3.(a). It follows by the contrapositive that $x\cdot y \neq 0$ implies $x \neq 0$ and $y \neq 0$.

Now suppose $x \neq 0$ and $y \neq 0$ and $x\cdot y = 0$. It follows that x^{-1} and y^{-1} both exist. We have

$$\begin{aligned} 1 &= 1\cdot 1 && (M4) \\ &= (x\cdot x^{-1})\cdot(y\cdot y^{-1}) && (M5,\ \text{twice}) \\ &= (x^{-1}\cdot y^{-1})\cdot(x\cdot y) && (M2 \text{ and } M3) \\ &= (x^{-1}\cdot y^{-1})\cdot 0 && (\text{assumption}) \\ &= 0 && (3.(a)). \end{aligned}$$

Since this cannot be from $3(b)$, it follows that $x \neq 0$ and $y \neq 0$ implies $x\cdot y \neq 0$, which completes the proof.

3.(d): For every $x, y \in \mathbb{F}$, we have

$$\begin{aligned} x\cdot y + (-x)\cdot y &= (x + (-x))\cdot y && (D) \\ &= 0\cdot y && (A5) \\ &= 0 && (3.(a)). \end{aligned}$$

It follows by (A5) and property 1.(a) that $x\cdot y$ is the inverse of $(-x)\cdot y$, i.e. we have $(-x)\cdot y = -(x\cdot y)$. The other half follows similarly.

3.(e): For every $x, y \in \mathbb{F}$, we have

$$\begin{aligned}(-x)\cdot(-y) &= -(x\cdot(-y)) && (3.(d))\\ &= -(-(x\cdot y)) && (3.(d))\\ &= x\cdot y && (1.(c))\end{aligned}$$

and we are done. □

This has certainly been a lot of work, but think about what we have accomplished. We have shown that the traditional rules of arithmetic, as we normally understand them, follow from a few basic axioms. In order to have the whole power afforded by having fields, all we have to do is verify a few basic axioms!

We can combine the notion of a field to our established order operator to get the following.

Definition 3.2 (Definition 1.17 in Rudin)**.** *A field $\mathbb{F}$ is called an **ordered field** if it has an order operator $<$ which satisfies:*

(OF1) For all $x, y, z \in \mathbb{F}$, if $y < z$ then $x + y < x + z$; and

(OF2) For all $x, y \in \mathbb{F}$, if $x > 0$ and $y > 0$ then $x \cdot y > 0$.

These axioms are sufficient to guarantee many of the order properties we have had drilled into us since grade school. For instance, we can show that

1. $x > 0$ iff $-x < 0$;
2. $x > 0$ and $y > z$ implies $xy > xz$;
3. $x^2 > 0$ for all $x \in \mathbb{F}$;
4. $1 > 0$; and
5. $0 < x < y$ iff $0 < y^{-1} < x^{-1}$.

We will not prove these results here (they can be found in Rudin).

We should probably pause to consider a few examples.

Example 1: The $\mathbb{R}$ and $\mathbb{Q}$ are ordered fields.

Justification: All of the required axioms (A1-5), (M1-5), (D), and (OF1-2) are classical for $\mathbb{R}$ and so the details are omitted. It is worth noting that $x^{-1} = (1/x)$.

For $\mathbb{Q}$, we have a little more work to do. We can check that, for $x = a/b \in \mathbb{Q}$ and $y = p/q \in \mathbb{Q}$ (where $a, b, p, q \in \mathbb{Z}$), we have that

$$x + y = \frac{a}{b} + \frac{p}{q} = \frac{aq + bp}{bq} \in \mathbb{Q}$$

and

$$xy = \frac{a}{b}\frac{p}{q} = \frac{ap}{bq} \in \mathbb{Q}$$

so that the operations satisfy the closure properties (A1) and (M1). The associativity, commutativity, and identity properties are trivial, as is the inverse property for addiction. For multiplication, we can clearly see that, for any $x = a/b \in \mathbb{Q}$, we have

$$x \cdot x^{-1} = \frac{a}{b}\frac{b}{a} = 1$$

so that $x^{-1} = b/a \in \mathbb{Q}$ is the desired inverse. Since the distributive law and order properties clearly hold for rational numbers, we are done.

Example 2: The natural numbers $\mathbb{N}$ and integers $\mathbb{Z}$ are not fields.

Justification: It suffices to show that any one of the axioms fails. For the natural numbers $\mathbb{N}$, we encounter a problem with the identity element, since there is no element $0 \in \mathbb{N}$ so that $n + 0 = n$ for all $n \in \mathbb{N}$ (because $0 \notin \mathbb{N}$). It is also clear that the additive inverse property fails, since there are no negative numbers, so that there is no $-n \in \mathbb{N}$ such that $n + (-n) = 0$ for a given $n \in \mathbb{N}$. It follows that $\mathbb{N}$ is not a field.

Now consider the integers $\mathbb{Z}$. We do not have the problems with additive identity and inverses, since $0 \in \mathbb{Z}$ and for every $x \in \mathbb{Z}$, we have $-x \in \mathbb{Z}$ so that $x + (-x) = 0$. Consider, however, the *multiplicative* identity and inverse properties. We clearly have that $1 \in \mathbb{Z}$ and $x \cdot 1 = x$ for all $x \in \mathbb{Z}$. Consider, however, the expression $x \cdot x^{-1} = 1$. Say we pick $x = 2$ (any number will do). The inverse we want to pick is $x^{-1} = 1/2$ but $1/2 \notin \mathbb{Z}$. It follows that the integers do not have a multiplicative inverse, and therefore are not a field.

Note: It is worth pointing out that the field axioms are fairly strong, as even the very common numerical systems $\mathbb{N}$ and $\mathbb{Z}$ fail them. There are weaker but also very useful notions in *abstract algebra* known as **groups** and **rings**. These notions contain some, but not all, of the field axioms.

4 Other Fields

The examples of $\mathbb{Q}$ and $\mathbb{R}$ are slightly trivial since the addition and multiplication operations are exactly what we traditionally understand them to be. For a (slightly) non-trivial example, consider the set of ordered pairs

$$S = \{(a, b) \mid a, b \in \mathbb{R}\}. \tag{1}$$

Note that by *ordered pair* we mean that (a, b) is a different object than (b, a) (unless $a = b$). That is to say, order matters. We *do not* mean that it is an ordered set!

Now consider the elements $x = (a, b)$ and $y = (c, d)$ and define the addition operator

$$x + y = (a + b, c + d) \tag{2}$$

and the multiplication operator

$$x \cdot y = (ac - bd, ad + bc). \tag{3}$$

The additional operation certainly looks like what we might expect, but the multiplication operator is, at first glance, somewhat bewildering. (We will see in a moment that it has a natural correspondence with a system we known very well!) At any rate, the following result holds.

Theorem 4.1 (Theorem 1.25 in Rudin)**.** *The set S defined by (4.1) together with addition operator (2) and multiplication operator (3) forms a field with additive identity $(0, 0) \in S$ and multiplicative identity $(1, 0) \in S$. Furthermore, for each $x = (a, b) \in S$, the additive inverse is $-x = (-a, -b) \in S$ and the multiplicative inverse is*

$$x^{-1} = \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right).$$

Proof. We omit the details of most of the proof, which can be found on page 13 of Rudin. (A1-A5) are straight forward, as is (M1). The multiplicative identities require a little more work. The most bewildering of the principles is probably the multiplicative inverse (M5). However, it is easily to check that, for $x = (a, b)$ and the given x^{-1}, we have

$$\begin{aligned} x \cdot x^{-1} &= (a, b) \cdot \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right) \\ &= \left(a \cdot \frac{a}{a^2 + b^2} - b \cdot \frac{-b}{a^2 + b^2}, a \cdot \frac{-b}{a^2 + b^2} + b \cdot \frac{a}{a^2 + b^2} \right) \\ &= (1, 0) \end{aligned}$$

where we recognize $(1, 0)$ as the multiplicative identity element. $\square$

While this is certainly a non-trivial example on the face of it, we could certainly be accused of playing sleight of hand. The operations (2) and (3) defined above are actually the operations of addition and multiplication as traditionally defined for *complex* numbers, i.e. numbers of the form

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}, i = \sqrt{-1}\}$$

if we treat $x = a + bi$ as the ordered pair $x = (a, b)$. The equivalence can be noted by recalling that $i \cdot i = \sqrt{-1} \cdot \sqrt{-1} = -1$. It then follows immediately that, for $x = a + bi$ and $y = c + di$, we have

$$x + y = (a + bi) + (c + di) = (a + c) + (b + d)i$$

and

$$x \cdot y = (a + bi) \cdot (c + di) = ac + (ad + bc)i + bci^2 = (ac - bc) + (ad + bc)i.$$

The additive identity element in Theorem 4.1 is simply $(0) + (0)i = 0$ while the multiplicative identity is $(1) + (0)i = 1$. We should note also that $\mathbb{R} \subseteq \mathbb{C}$ since any $x \in \mathbb{R}$ can be thought of as the complex number $z = x + (0)i \in \mathbb{C}$.

We might wonder where the multiplicative inverse comes from in the context of this realization. For $x = a + bi$, we want to define

$$x^{-1} = \frac{1}{a + bi}.$$

While this looks good at first glance there is the problem that z^{-1} is not in the form of a complex number. The trick to corresponding this form to that previous form is to rationalize the denominator:

$$z^{-1} = \frac{1}{a + bi} \cdot \left(\frac{a - bi}{a - bi}\right) = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

We have already verified that this is the correct multiplicative inverse! Notice also that this inverse may only fail to be defined if $a^2 + b^2 = 0$, i.e. if $a = b = 0$. That is to say, the only element without an inverse is $z = (0) + (0)i = 0$ which we recognize as the additive identity.

The long and the short of this whole discussion is that the set of complex numbers $\mathbb{C}$ together with the standard additional and multiplication operators form a field. It is also worth noting that, whenever we consider the complex numbers $\mathbb{C}$, it will be sufficient to consider that set of ordered pairs (a, b) where $a, b \in \mathbb{R}$. We will define this space more generally in a week or two.