Introduction

1 Notation

If X is a set, we write $x \in X$ to mean that x is an element of X, and $x \notin X$ to mean that x is not an element of X.

Suppose X and Y are sets. We say that X is a *subset* of Y, denoted $X \subseteq Y$, if every element of X is also an element of Y. We say that $X = Y$ if both $X \subseteq Y$ and $Y \subseteq X$. In other words, $X = Y$ if and only if X and Y have exactly the same elements. Finally, we say that X is a *proper subset* of Y, denoted $X \subsetneq Y$, if $X \subseteq Y$ but there exists some element of Y which is not in X.

We write $\emptyset$ to denote the *empty set*, which is the set containing no elements.

2 Rationals

When people develop the foundations of mathematics, there's basically an axiom that says that the set $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ of natural numbers exists. Then they perform various set-theoretic operations to construct the larger set $\mathbb{Z}$ of *integers*, which include the numbers $-1, -2, -3, \dots$ in addition to the natural numbers. Then another construction expands this further to the set $\mathbb{Q}$ of *rational numbers*, which are numbers of the form a/b where a and b are integers with b nonzero. I'm going to skip all of that foundational work and assume that you know how to work with rational numbers. Let me just point out some salient properties of the rational numbers.

- A rational number is not exactly the same thing as a numerator-denominator pair: for example, the rational numbers $1/2$ and $2/4$ are the same, even though one has numerator 1 and the other has numerator 2.

- We can add, subtract and multiply rational numbers and the result is still rational. Also, we can divide rationals by other nonzero rationals and the result is again still rational.

- Also we have an order on the rationals, and this order satisfies the nice property that between any two distinct rational numbers there is a third rational number.

Despite these nice properties, there are some problems with the rational numbers. Here are two related results indicating these problems. The reason we'll care about the real numbers is because they're going to solve these problems.

Lemma 2.1. *There exists no rational number x such that $x^2 = 2$.*

Proof. Suppose there did exist such a rational number $x = a/b$, where a and b are integers and b is nonzero. By writing this fraction in lowest terms, we can assume that a and b have no common factors. Now note that $x^2 = 2$ means that $a^2 = 2b^2$, which means that a^2 is even. But then a has to be even, so $a = 2c$ for some integer c. Then

$$4c^2 = 2b^2$$

which means that $b^2 = 2c^2$, so b^2 and therefore also b must be even. This is a contradiction: we have just shown that a and b are both even and therefore have a common factor of 2, but we had assumed that a and b had no common factors. □

Lemma 2.2. $\mathbb{Q}$ *does not have the supremum property.*

We'll now make a detour to define what it means to have the supremum property. We won't prove lemma 2.2 until later.

3 Ordered Sets

Let X be a set. A *(total) order* on X is a relation $\leq$ on X satisfying all of the following properties.

(O1) (Reflexivity) $x \leq x$ for every $x \in X$.

(O2) (Antisymmetry) If $x \leq y$ and $y \leq x$, then $x = y$.

(O3) (Transitivity) If $x \leq y$ and $y \leq z$, then $x \leq z$.

(O4) For any $x, y \in X$, we have either $x \leq y$ or $y \leq x$.

We also write $x \lneq y$ to mean that $x \leq y$ but $x \neq y$. An *ordered set* is a set X on which an order is defined. Let E be a subset of an ordered set X.

- An *upper bound* for E is an element $\alpha \in X$ such that $x \leq \alpha$ for all $x \in E$.
- If there exists an upper bound for E in X, then E is *bounded above.*
- If α is an upper bound for E, and it satisfies the further property that $\alpha \leq \alpha'$ for any upper bound α' of E, then α is called the *supremum* of E and is denoted $\sup E$.

We can analogously define the terms *lower bound*, *bounded below*, and *infimum*. The infimum of a set E is denoted $\inf E$. Sometimes, supremums are also called *least upper bounds* and infimums are analogously called *greatest lower bounds*. Also, a subset E is *bounded* if it is both bounded above and bounded below.

Example 3.1. It is easy to see that the usual order relation on the set $\mathbb{Q}$ of rational numbers satisfies all of the above properties, so $\mathbb{Q}$ is an ordered set. Consider the subset $E := \{1/n : n = 1, 2, \ldots\}$. Then 2 is an upper bound for E, but it is not the supremum since 1 is also an upper bound. In fact, $\sup E = 1$. Notice that $\sup E$ is actually an element of E. On the other hand, we have $\inf E = 0$. Clearly 0 is a lower bound for E. To see that it is the greatest lower bound, suppose that $r \gneq 0$ is a lower bound for E. Then we can write $r = a/n$ for some $a, n \in \mathbb{N} \smallsetminus \{0\}$, and we have

$$1/(n+1) \lneq 1/n \leq a/n = r.$$

Since $1/(n+1)$ is an element of E, this contradicts the fact that r was suppsed to be a lower bound for E. Thus $\inf E = 0$. Notice that $0 \notin E$.

For some more examples, consider the subsets $E_1 := \{x \in \mathbb{Q} : x \leq 0\}$ and $E_2 := \{x \in \mathbb{Q} : x \lneq 0\}$. Then

$$\sup E_1 = 0 = \sup E_2,$$

even though $0 \in E_1$ and $0 \notin E_2$. The take-away message from these examples is that the supremum and the infimum of a set can be, but need not be, contained in that set.

An ordered set X has the *supremum property* if every nonempty subset of X which is bounded above has a supremum in X. Now that we have this definition, we know what lemma 2.2 means: it's saying that there is some nonempty subset of $\mathbb{Q}$ which is bounded above but has no supremum. In fact, it turns out that the set

$$E := \{x \in \mathbb{Q} : x^2 \leq 2\}$$

is an example of such a set. You can find an elementary proof of this assertion in Rudin (combine example 1.1 and example 1.9(a)), but I find this proof extremely unenlightening (and I would be very much indebted if someone could explain to me conceptually how Rudin arrives at formula (3) in example 1.1). Instead, what we will do is deduce this after we have the real numbers.

One immediate question that one might ask is why we haven't introduced a "infimum property." It turns out that this is unnecessary.

Proposition 3.2. *Let X be an ordered set which has the supremum property and E a nonempty subset which is bounded below. Then E has an infimum.*

Proof. Let F be the set of lower bounds for E. Since E is bounded below, the set F is nonempty. Moreover, every element of E is an upper bound for F. Indeed, given an arbitrary $x \in E$, we see that for every $y \in F$ we have $y \leq x$ since F is a set of lower bounds for E, so x is an upper bound for F.

Since E is nonempty, it has some element and that element is an upper bound for F. In other words, we have just shown that F is nonempty and bounded above, so by the supremum property, it has a supremum α. We now claim that $\alpha = \inf E$. To see this, let us show first that α is a lower bound for E. Suppose for a contradiction that there exists some $x \in E$ such that $x \lneq \alpha$. Since $\alpha = \sup F$, and x is strictly less than α, we see that x cannot be an upper bound for F. But we saw above that every element of E was an upper bound for F, so this is a contradiction.

To finish the proof, we need to show that α is greater than any other lower bound β for E. But any such lower bound β is an element of F by definition, so $\beta \leq \sup F = \alpha$. Thus α is a lower bound for E which is greater than all other lower bounds for E, so it is the infimum of E. □

4 Fields

Aside from being able to compare elements of $\mathbb{Q}$, we can also add, substract, multiply and divide them. In other words, $\mathbb{Q}$ is an example of a mathematical structure called a field. A *field* is a set F, together with two binary operations $+$ and $\cdot$, called *addition* and *multiplication*, respectively, which satisfy all of the following axioms.

(F1) $+$ is associative: $(x+y)+z = x+(y+z)$ for all $x, y, z \in F$.

(F2) $+$ is commutative: $x+y = y+x$ for all $x, y \in F$.

(F3) F contains an element 0, called a *additive identity*, such that $0+x = x$ for all $x \in F$.

(F4) For every $x \in F$ there exists an element $-x \in F$, called the *additive inverse* of x, such that $x + (-x) = 0$.

(F5) $\cdot$ is associative: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in F$.

(F6) $\cdot$ is commutative: $x \cdot y = y \cdot x$ for all $x, y \in F$.

(F7) F contains an element 1, called a *multiplicative identity*, such that $1 \cdot x = x$ for all $x \in F$.

(F8) If $x \in F \setminus \{0\}$, then there exists an element $1/x$, called the *multiplicative inverse* of x, such that $x \cdot (1/x) = 1$.

(F9) Multiplication distributes over addition: $x \cdot (y+z) = x \cdot y + x \cdot z$ for any $x, y, z \in F$.

(F10) $0 \neq 1$.

If F is a field, we usually write $x-y$ in place of $x+(-y)$, and xy in place of $x \cdot y$, and x/y in place of $x \cdot (1/y)$, and x^2 in place of $x \cdot x$, and $2x$ in place of $x+x$, and so forth.

Example 4.1. $\mathbb{Q}$ is a field with the usual operations. All of the axioms above are standard properties that you are all used to. The set $\mathbb{N}$ is not a field: axioms (F4) and (F8) are not satisfied in $\mathbb{N}$. Axiom (F4) is satisfied in $\mathbb{Z}$, but (F8) is still not satisfied so $\mathbb{Z}$ is not a field either.

There are a lot of properties that we are familiar with for $\mathbb{Q}$ that are actually a formal consequence of the field axioms. Here is a long list of many of them. It is a good exercise to try to prove all of these using the axioms above: none of the proofs are difficult. If you find yourself getting stuck, some of these are proved in Rudin, propositions 1.14, 1.15 and 1.16.

Proposition 4.2. *Let F be a field. Then the following statements hold for all $x, y, z \in F$.*

(a) (Cancellation law for addition) If $x+y = x+z$, then $y = z$.

(b) (Uniqueness of the additive identity) If $x+y = x$, then $y = 0$.

(c) (Uniqueness of additive inverses) If $x+y = 0$, then $y = -x$.

(d) $-(-x) = x$.

(e) (Cancellation law for multiplication) If $x \neq 0$ *and* $xy = xz$, *then* $y = z$.

(f) (Uniqueness of the multiplicative identity) If $x \neq 0$ *and* $xy = x$, *then* $y = 1$.

(g) (Uniqueness of multiplicative inverses) If $x \neq 0$ *and* $xy = 1$, *then* $y = 1/x$.

(h) $1/(1/x) = x$.

(i) $0 \cdot x = 0$.

(j) If $x \neq 0$ *and* $y \neq 0$, *then* $xy \neq 0$.

(k) $(-x)y = -(xy)$.

(l) $(-x)(-y) = xy$.

5 Ordered Fields

We saw above that $\mathbb{Q}$ is an ordered set, and then that it is a field. These two structures interact in particular ways. We're now going to define a structure called an ordered field which axiomatizes the interaction between order and the field operations. An *ordered field* is a field F equipped with an order $\leq$ such that the following axioms are satisfied.

(OF1) If $x, y, z \in F$ and $x \leq y$, then $x + z \leq y + z$.

(OF2) If $x, y \in F$ and $0 \leq x$ and $0 \leq y$, then $0 \leq xy$.

Again, many of the properties we are used to with $\mathbb{Q}$ are actually formal consequences of the axioms for an ordered field. Here are some of them. The proofs of these assertions are also excellent exercises. If you get stuck, you can find the proof of some of these in Rudin, proposition 1.18.

Proposition 5.1. *Let* F *be an ordered field. Then the following statements hold for all* $x, y, z \in F$.

(a) If $x \geq 0$, *then* $-x \leq 0$, *and vice versa.*

(b) If $x \geq 0$ *and* $y \leq z$, *then* $xy \leq xz$.

(c) If $x \leq 0$ *and* $y \leq z$, *then* $xy \geq xz$.

(d) If $x \neq 0$, *then* $x^2 \gneq 0$.

(e) $1 \geq 0$.

(f) If $0 \lneq x \leq y$, *then* $0 \lneq 1/y \leq 1/x$.

Proposition 5.2. *Let* F *be an ordered field. Then* F *contains* $\mathbb{Q}$ *as a subfield.*

The following proof is "optional" because it will likely only make sense to you if you're familiar with the concept of the "characteristic" of a field. Don't worry about understanding the proof if you don't know what this means.

Optional proof. It is sufficient to show that F is of characteristic 0. We claim that

$$\overbrace{1+\cdots+1}^{n\text{ times}} =: n \gneq 0$$

for all positive integers n. We do this by induction, with the base case being a combination of proposition 5.1(e) and the non-degeneracy axiom (F10) for fields. Inductively, suppose $n \gneq 0$. Then (OF1) tells us that $n+1 \geq 1$, and $1 \geq 0$ by proposition 5.1(e) again, so by the transitivity axiom (O3) we get $n+1 \geq 0$. If $n+1 = 0$, then

$$0 \leq 1 \leq n+1 \leq 0$$

which means, by the transitivity axiom (O3), that $1 \leq 0$. In other words, since we have both $1 \leq 0$ and $0 \leq 1$, by the antisymmetry axiom (O2) we get $1 = 0$. This contradicts the non-degeneracy axiom (F10) for fields. Thus $n+1 \neq 0$, so $n+1 \gneq 0$, completing the induction. □

6 Sample Problems

Problem 1. Show that there exists no rational number whose cube is 6.

Solution. Suppose there did exist a rational number a/b whose cube is 6. Let us assume that a and b have no common factors. Clearing denominators from the equation $(a/b)^3 = 6$, we find that $6b^3 = a^3$. Since 6 is even, so is $6b^3$, so a^3 is even. But the cube of an odd number is always odd, so in order for a^3 to be even, a must be even. This means that we can write $a = 2c$ for some $c \in \mathbb{Z}$, and then

$$6b^3 = a^3 = (2c)^3 = 8c^3.$$

Diving this equation through by 2, we find that $3b^3 = 4c^3$. But now 4 is even, so $4c^3$ is even, so $3b^3$ is even. But 3 is odd, so in order for $3b^3$ to be even we must have that b^3 is even, which in turn implies that b is even. But then both a and b are even, which is a contradiction. □

Problem 2. Let F be a field. If $x, y, z \in F$, $x \neq 0$ and $xy = xz$, show that $y = z$.

Solution. Since $x \neq 0$, by axiom (F8) there exists $1/x \in F$ such that $x(1/x) = 1$. By the commutativity axiom (F6), we have $(1/x)x = 1$ as well. Then

$$y \overset{\text{(F7)}}{=} 1 \cdot y = ((1/x)x)y \overset{\text{(F5)}}{=} (1/x)\cdot(xy) = (1/x)\cdot(xz) \overset{\text{(F5)}}{=} ((1/x)x)z = 1 \cdot z \overset{\text{(F7)}}{=} z. \qquad □$$

Problem 3. Let F be an ordered field. If $x \geq 0$ and $y \leq z$ for some $x, y, z \in F$, show that $xy \leq xz$.

Solution. By (OF1), we have that

$$0 = y + (-y) \leq z + (-y) = z - y.$$

Then by (OF2) we see that $0 \leq x(z-y) = xz - xy$, using distributivity (F9) and the fact that $x(-y) = -xy$. (You should be able to prove this fact yourself! If you get stuck, check the proof of proposition 1.16(c) in Rudin.) But then, using (OF1) again, we see that

$$xy = 0 + xy \leq (xz - xy) + xy = xz + ((-xy) + xy) = xz + 0 = xz$$

using associativity of addition (F1), the additive inverse property (F4), and the additive identity property (F3). □