MATH 16210 (Honors Calculus II IBL) Notes

Steven Labalme

February 4, 2021

Contents

Script 6

Construction of the Real Numbers

6.1 Journal

1/12: **Definition 6.1.** A subset A of $\mathbb{Q}$ is said to be a **cut** (or **Dedekind cut**) if it satisfies the following:

(a) $A \neq \emptyset$ and $A \neq \mathbb{Q}$.

(b) If $r \in A$ and $s \in \mathbb{Q}$ satisfy $s < r$, then $s \in A$.

(c) A does not have a last point; i.e., if $r \in A$, then there is some $s \in A$ with $s > r$.

We denote the collection of all cuts by $\mathbb{R}$.

Lemma 6.2. *Let A be a Dedekind cut and $x \in \mathbb{Q}$. Then $x \notin A$ if and only if x is an upper bound for A.*

Proof. Suppose first that x is an element of $\mathbb{Q}$ such that $x \notin A$. To prove that x is an upper bound for A, Definition 5.6 tells us that it will suffice to show that for all $r \in A$, $r \leq x$. Let r be an arbitrary element of A. Then since $r \in A$, $x \in \mathbb{Q}$, and $x \notin A$, the contrapositive of Definition 6.1b asserts that $x \not< r$. Therefore, $r \leq x$, as desired.

Now suppose that x is an upper bound for A. By Definition 5.6, this implies that for all $r \in A$, $r \leq x$. Therefore, since there is no $r \in A$ with $r > x$, by the contrapositive of Definition 6.1c, $x \notin A$, as desired. ☐

Exercise 6.3.

(a) Prove that for any $q \in \mathbb{Q}$, $\{x \in \mathbb{Q} \mid x < q\}$ is a Dedekind cut. We then define $\mathbf{0} = \{x \in \mathbb{Q} \mid x < 0\}$.

(b) Prove that $\{x \in \mathbb{Q} \mid x \leq 0\}$ is not a Dedekind cut.

(c) Prove that $\{x \in \mathbb{Q} \mid x < 0\} \cup \{x \in \mathbb{Q} \mid x^2 < 2\}$ is a Dedekind cut.

Proof of a. Let q be an arbitrary element of $\mathbb{Q}$. To prove that $A = \{x \in \mathbb{Q} \mid x < q\}$ is a Dedekind cut, Definition 6.1 tells us that it will suffice to show that $A \neq \emptyset$; $A \neq \mathbb{Q}$; if $r \in A$ and $s \in \mathbb{Q}$ satisfy $s < r$, then $s \in A$; and if $r \in A$, then there is some $s \in A$ with $s > r$. We will take this one claim at a time.

To show that $A \neq \emptyset$, Definition 1.8 tells us that it will suffice to find an element of A. By Exercise 3.9d, q is not the first point of $\mathbb{Q}$. Thus, by Definition 3.3, there exists an object $x \in \mathbb{Q}$ such that $x < q$. By the definition of A, this implies that $x \in A$, as desired.

To show that $A \neq \mathbb{Q}$, Definition 1.2 tells us that it will suffice to find an element of $\mathbb{Q}$ that is not an element of A. By hypothesis, $q \in \mathbb{Q}$. By Exercise 3.9d, $q \not< q$. Therefore, $q \in \mathbb{Q}$ but $q \notin A$, as desired.

To show that if $r \in A$ and $s \in \mathbb{Q}$ satisfy $s < r$, then $s \in A$, we let $r \in A$ and $s \in \mathbb{Q}$ be arbitrary elements of their respective sets that satisfy $s < r$ and seek to verify that $s \in A$. Since $r \in A$, $r < q$. This combined with the fact that $s < r$ implies by transitivity that $s < q$. Therefore, since $s \in \mathbb{Q}$ and $s < q$, $s \in A$, as desired.

To show that if $r \in A$, then there is some $s \in A$ with $s > r$, we let $r \in A$ and seek to find such an s. By the definition of A, $r < q$. Thus, by Additional Exercise 3.1, there exists a point $s \in \mathbb{Q}$ such that $r < s < q$. Since $s \in \mathbb{Q}$ and $s < q$, $s \in A$. It follows that s is the desired element of A which satisfies $s > r$. ☐

Proof of b. To prove that $A = \{x \in \mathbb{Q} \mid x \leq 0\}$ is not a Dedekind cut, Definition 6.1 tells us that it will suffice to show that A *does* have a last point. To show this, we will demonstrate that 0 is the last point of A. To demonstrate this, Definition 3.1 tells us that it will suffice to confirm that $0 \in A$ and for all $x \in A$, $x \leq 0$. Since $0 \leq 0$ and $0 \in \mathbb{Q}$, $0 \in A$. Additionally, by the definition of A, it is true that for all $x \in A$, $x \leq 0$. □

Proof of c. Let $B = \{x \in \mathbb{Q} \mid x < 0\}$ and let $C = \{x \in \mathbb{Q} \mid x^2 < 2\}$. To prove that $A = B \cup C$ is a Dedekind cut, Definition 6.1 tells us that it will suffice to show that $A \neq \emptyset$; $A \neq \mathbb{Q}$; if $r \in A$ and $s \in \mathbb{Q}$ satisfy $s < r$, then $s \in A$; and if $r \in A$, then there is some $s \in A$ with $s > r$. We will take this one claim at a time.

To show that $A \neq \emptyset$, Definition 1.8 tells us that it will suffice to find an element of A. Since $-1 \in \mathbb{Q}$ and $-1 < 0$, $-1 \in B$. Therefore, by Definition 1.5, $-1 \in A$, as desired.

To show that $A \neq \mathbb{Q}$, Definition 1.2 tells us that it will suffice to find an element of $\mathbb{Q}$ that is not an element of A. Since $2 \geq 0$, $2 \notin B$. Additionally, since $2^2 \geq 2$, $2 \notin C$. Therefore, by Definition 1.5, $2 \notin A$, as desired.

To show that if $r \in A$ and $s \in \mathbb{Q}$ satisfy $s < r$, then $s \in A$, we let $r \in A$ and $s \in \mathbb{Q}$ be arbitrary elements of their respective sets that satisfy $s < r$ and seek to verify that $s \in A$. We divide into two cases ($s < 0$ and $s \geq 0$). Suppose first that $s < 0$. Then $s \in B$, meaning that $s \in A$. Now suppose that $s \geq 0$. Then by Script 0, we have $0 \leq s^2 < r^2 < 2$. Thus, by the definition of C, $s \in C$, implying that $s \in A$.

To show that A does not have a last point, suppose for the sake of contradiction that A has a last point p. We now divide into two cases ($p \leq 0$ and $p > 0$). Suppose first that $p \leq 0$. Since p is the last point of A, Definition 3.3 tells us that $x \leq p$ for all $x \in A$. But $1 \in A$ (since $1 \in \mathbb{Q}$ and $1^2 = 1 < 2$ implies $1 \in B$, implies $1 \in A$) and $1 > 0 \geq p$, a contradiction. Now suppose that $p > 0$. Definition 3.3 tells us that $p \in A$, but the condition that $p > 0$ means $p \notin B$, so we must have $p \in C$. However, by the proof of Exercise 4.24, $\frac{2(p+1)}{p+2}$ will be an element of B (and therefore A) that is greater than p no matter how large p is, a contradiction. □

Definition 6.4. If $A, B \in \mathbb{R}$, we say that $A < B$ if A is a proper subset of B.

Exercise 6.5. Show that $\mathbb{R}$ satisfies Axioms 1, 2, and 3.

Proof. By Exercise 6.3a, $\{x \in \mathbb{Q} \mid x < 0\} \in \mathbb{R}$ since $0 \in \mathbb{Q}$. Therefore, Axiom 1 is immediately satisfied.

Axiom 2 asserts that $\mathbb{R}$ must have an ordering $<$. As such, it will suffice to verify that the ordering given by Definition 6.4 satisfies the stipulations of Definition 3.1. To prove that $<$ satisfies the trichotomy, it will suffice to show that for all $A, B \in \mathbb{R}$, exactly one of the following holds: $A < B$, $B < A$, or $A = B$.

We first show that *no more than one* of the three statements can simultaneously be true. Let A, B be arbitrary elements of $\mathbb{R}$. We divide into three cases. First, suppose for the sake of contradiction that $A < B$ and $B < A$. By Definition 6.4, this implies that $A \subsetneq B$ and $B \subsetneq A$. Thus, by Definition 1.3, $A \subset B$, $B \subset A$, and $A \neq B$. But by Theorem 1.7, $A \subset B$ and $B \subset A$ implies that $A = B$, a contradiction. Second, suppose for the sake of contradiction that $A < B$ and $A = B$. By substitution, we have that $A < A$. But by Definitions 6.4 and 1.3, it follows that $A \neq A$. The proof of the third case ($B < A$ and $A = B$) is symmetric to that of the second case.

We now show that *at least one* of the three statements is always true. Let A, B be arbitrary elements of $\mathbb{R}$, and suppose for the sake of contradiction that $A \not< B$, $B \not< A$, and $A \neq B$. Since $A \not< B$ and $B \not< A$, we have by Definition 6.4 that $A \not\subsetneq B$ and $B \not\subsetneq A$. Thus, by Definition 1.3, $A \not\subset B$ or $A = B$, and $B \not\subset A$ or $A = B$. But $A \neq B$ by hypothesis, so it must be that $A \not\subset B$ and $B \not\subset A$. It follows from the first statement by Definition 1.3 that there exists an object $x \in A$ such that $x \notin B$, and there exists an object $y \in B$ such that $y \notin A$. Since $x \notin B$, Lemma 6.2 implies that x is an upper bound of B. Consequently, by Definition 5.6, $p \leq x$ for all $p \in B$, including y. Similarly, $p \leq y$ for all $p \in A$, including x. Thus, we have $y \leq x$ and $x \leq y$, implying that $x = y$. But since $y \in B$, this implies that $x \in B$, a contradiction.

To prove that $<$ is transitive, it will suffice to show that for all $A, B, C \in \mathbb{R}$, if $A < B$ and $B < C$, then $A < C$. Let A, B, C be arbitrary elements of $\mathbb{R}$ for which it is true that $A < B$ and $B < C$. By Definition 6.4, we have $A \subsetneq B$ and $B \subsetneq C$. Thus, by Script 1, $A \subsetneq C$. Therefore, by Definition 6.4, $A < C$.

Axiom 3 asserts that $\mathbb{R}$ must have no first or last point. We will take this one argument at a time

Suppose for the sake of contradiction that $\mathbb{R}$ has some first point A. Then by Definition 3.3, $A \leq X$ for every $X \in \mathbb{R}$. Now since A is a Dedekind cut, Definition 6.1 tells us that $A \neq \emptyset$. Thus, by Definition 1.8, there exists some $q \in A$. Additionally, $A \subset \mathbb{Q}$ by Definition 6.1, so $q \in A$ implies that $q \in \mathbb{Q}$. It follows by Exercise 6.3a that $B = \{x \in \mathbb{Q} \mid x < q\}$ is a Dedekind cut. We now seek to prove that $B \subsetneq A$. To do this, Definition 1.3 tells us that it will suffice to show that $B \neq A$ and $B \subset A$. To show that $B \neq A$, Definition 1.2 tells us that it will suffice to find an element of A that is not an element of B. Conveniently, q is clearly such an object. To show that $B \subset A$, Definition 1.3 tells us that we must confirm that every element of B is an element of A. Let p be an arbitrary element of B. Then by the definition of B, $p \in \mathbb{Q}$ and $p < q$. It follows by Definition 6.1b (which clearly applies to A) that $p \in A$, as desired. Having proven that $B \subsetneq A$, Definition 6.4 tells us that $B < A$. But this contradicts the previously demonstrated fact that $A \leq X$ for every $X \in \mathbb{R}$, including B.

Suppose for the sake of contradiction that $\mathbb{R}$ has some last point A. Then by Definition 3.3, $X \leq A$ for every $X \in \mathbb{R}$. Now since A is a Dedekind cut, Definition 6.1 tells us that $A \neq \mathbb{Q}$. Thus, by Definition 1.2, there exists some $q \in \mathbb{Q}$ such that $q \notin A$. It follows by Lemma 6.2 that q is an upper bound of A. Consequently, by Definition 5.6, $x \leq q$ for all $x \in A$. Additionally, by Exercise 6.3a, $B = \{x \in \mathbb{Q} \mid x < q + 1\}$[1] is a Dedekind cut. We now seek to prove that $A \subsetneq B$. As before, this means we must show that $A \neq B$ and $A \subset B$. To show that $A \neq B$, Definition 1.2 tells us that it will suffice to find an element of B that is not an element of A. Since $x \leq q$ for all $x \in A$ and $q < q + 0.5 < q + 1$, $q + 0.5 \notin A$ and $q + 0.5 \in B$ is one such desired object. To show that $A \subset B$, Definition 1.3 tells us that we must confirm that every element of A is an element of B. Let p be an arbitrary element of A. As an element of A, we know that $p \leq q$. Thus, $p < q + 1$, so $p \in B$, as desired. Having proven that $A \subsetneq B$, Definition 6.4 tells us that $A < B$. But this contradicts the previously demonstrated fact that $X \leq A$ for every $X \in \mathbb{R}$, including B. ☐

1/14: **Lemma 6.6.** *A nonempty subset of $\mathbb{R}$ that is bounded above has a supremum.*

Proof. Let X be an arbitrary nonempty subset of $\mathbb{R}$ that is bounded above. To prove that $\sup X$ exists, we will show that $\sup X = U = \bigcup\{Y \mid Y \in X\}$. To show this, Definition 5.7 tells us that it will suffice to demonstrate that $U \in \mathbb{R}$, U is an upper bound of X, and if U' is an upper bound of X, then $U \leq U'$. Let's begin.

To demonstrate that $U \in \mathbb{R}$, Definition 6.1 tells us that it will suffice to confirm that $U \neq \emptyset$; $U \neq \mathbb{Q}$; if $r \in U$ and $s \in \mathbb{Q}$ satisfy $s < r$, then $s \in U$; and if $r \in U$, then there is some $s \in U$ with $s > r$.

As the union of a nonempty set of nonempty sets, Script 1 implies that $U \neq \emptyset$.

To demonstrate that $U \neq \mathbb{Q}$, Definition 1.2 tells us that it will suffice to find a point $p \in \mathbb{Q}$ such that $p \notin U$. Since X is bounded above, we have by Definition 5.6 that there exists a Dedekind cut $V \in \mathbb{R}$ such that $A \leq V$ for all $A \in X$. It follows by Definition 6.4 that $A \subset V$ for all $A \in X$. Thus, by Script 1, $U \subset V$. Now since V is a Dedekind cut, we know by Definition 6.1 that $V \subset \mathbb{Q}$ and $V \neq \mathbb{Q}$, meaning that there exists a point $p \in \mathbb{Q}$ such that $p \notin V$. Consequently, since $U \subset V$, $p \notin U$, as desired.

To demonstrate that if $r \in U$ and $s \in \mathbb{Q}$ satisfy $s < r$, then $s \in U$, we let $r \in U$ and $s \in \mathbb{Q}$ be arbitrary elements of their respective sets that satisfy $s < r$ and seek to verify that $s \in U$. Since $r \in U$, Definition 1.13 tells us that $r \in A$ for some $A \in X$. Thus, since A is a Dedekind cut, $s \in \mathbb{Q}$ and $s < r$ implies that $s \in A$. Therefore, $s \in U$.

To demonstrate that if $r \in U$, then there is some $s \in U$ with $s > r$, we let $r \in U$ and seek to find such an s. Since $r \in U$, Definition 1.13 tells us that $r \in A$ for some $A \in X$. Thus, since A is a Dedekind cut, there exists a point $s \in A$ with $s > r$. Therefore, $s \in U$.

To demonstrate that U is an upper bound of X, Definition 5.6 tells us that it will suffice to confirm that $A \leq U$ for all $A \in X$. To confirm this, Definition 6.4 tells us that it will suffice to verify that $A \subset U$ for all $A \in X$. But by an extension of Theorem 1.7b, this is true.

Now suppose for the sake of contradiction that there exists an upper bound U' of X such that $U' < U$. It follows by Definitions 6.4 and 1.3 that there exists a point $p \in U$ such that $p \notin U'$. Thus, by the former statement and Definition 1.13, $p \in A$ for some $A \in X$. Additionally, since U' is an upper bound of X, we have by Definitions 5.6 and 6.4 that $A \subset U'$ for all $A \in X$. But this implies by Definition 1.3 that $p \in U'$, a contradiction. ☐

[1] Note that we add 1 to q to treat the case that $q = \sup A$, a case in which we would have $B = A$ if B were defined as $\{x \in \mathbb{Q} \mid x < q\}$.

1/19: **Exercise 6.7.** Show that $\mathbb{R}$ satisfies Axiom 4.

Proof. Suppose for the sake of contradiction that $\mathbb{R}$ does not satisfy Axiom 4. It follows that $\mathbb{R}$ is not connected, implying by Definition 4.22 that $\mathbb{R} = A \cup B$ where A, B are disjoint, nonempty, open sets. Since A, B are disjoint and nonempty, we know that there exist distinct objects $a \in A$ and $b \in B$. WLOG, let $a < b$.

We now seek to prove that the set $A \cap \underline{ab}$ is nonempty and bounded above. To prove that $A \cap \underline{ab}$ is nonempty, Definition 1.8 tells us that it will suffice to find an element of $A \cap \underline{ab}$. Since $a \in A$ and A is open, we have by Theorem 4.10 that there exists a region $\underline{cd}$ such that $a \in \underline{cd}$ and $\underline{cd} \subset A$. It follows by Definitions 3.10 and 3.6 that $a < d$, implying by Lemma 6.10[2] that there exists some point $x \in \mathbb{R}$ such that $c < a < x < d < b$ (note that $d < b$ since if $b < d$, then $b \in \underline{cd}$ would contradict the fact that $\underline{cd} \subset A$). Consequently, $x \in \underline{cd}$, meaning that $x \in A$, and $x \in \underline{ab}$. Therefore, $x \in A \cap \underline{ab}$, as desired. To prove that $A \cap \underline{ab}$ is bounded above, Definition 5.6 tells us that it will suffice to show that b is an upper bound of $A \cap \underline{ab}$. To show this, Definition 5.6 tells us that it will suffice to confirm that $y \leq b$ for all $y \in A \cap \underline{ab}$. Let y be an arbitrary element of $A \cap \underline{ab}$. Then by Definition 1.6, $y \in A$ and $y \in \underline{ab}$. It follows from the latter statement by Definitions 3.10 and 3.6 that $y < b$, i.e., $y \leq b$, as desired.

Having established that $A \cap \underline{ab} \subset \mathbb{R}$ is nonempty and bounded above, we can invoke Lemma 6.6 to learn that $A \cap \underline{ab}$ has a supremum $\sup(A \cap \underline{ab})$. We now divide into two cases ($\sup(A \cap \underline{ab}) \in A$ and $\sup(A \cap \underline{ab}) \in B$; it follows from the definitions of A and B that exactly one of these cases is true). Suppose first that $\sup(A \cap \underline{ab}) \in A$. Then since A is open, we have by Theorem 4.10 that there exists a region $\underline{ef}$ such that $\sup(A \cap \underline{ab}) \in \underline{ef}$ and $\underline{ef} \subset A$. It follows from the former condition that $\sup(A \cap \underline{ab}) < f$. Thus, by Lemma 6.10, there exists an object $z \in \mathbb{R}$ such that $e < \sup(A \cap \underline{ab}) < z < f < b$ (note that $f < b$ for the same reason that $d < b$). Consequently, $z \in \underline{ef}$, implying that $z \in A$, and $z \in \underline{ab}$. Thus, we have found an element of $A \cap \underline{ab}$ that is greater than $\sup(A \cap \underline{ab})$, contradicting Definitions 5.7 and 5.6. The proof is symmetric in the other case (except that we find an element of B less than $\sup(A \cap \underline{ab})$). $\square$

1/14: **Definition 6.8.** Let C be a continuum satisfying Axioms 1-4. Consider a subset $X \subset C$. We say that X is **dense** in C if every $p \in C$ is a limit point of X.

Lemma 6.9. *A subset $X \subset C$ is dense in C if and only if $\overline{X} = C$.*

Proof. Suppose first that $X \subset C$ is dense in C. To prove that $\overline{X} = C$, Definition 1.2 tells us that it will suffice to show that every point $p \in \overline{X}$ is an element of C and vice versa. Clearly, every element of $\overline{X}$ is an element of C. On the other hand, let p be an arbitrary element of C. Since X is dense in C, Definition 6.8 tells us that $p \in LP(X)$. Therefore, by Definitions 1.5 and 4.4, $p \in \overline{X}$.

Now suppose that $\overline{X} = C$. To prove that X is dense in C, Definition 6.8 tells us that it will suffice to show that every $p \in C$ is a limit point of X. Let p be an arbitrary element of C. By Corollary 5.4, this implies that $p \in LP(C)$. It follows that $p \in LP(\overline{X})$. Thus, by Definition 4.4, $p \in LP(X \cup LP(X))$. Consequently, by Theorem 3.20, $p \in LP(X)$ or $p \in LP(LP(X))$. We now divide into two cases. If $p \in LP(X)$, then we are done. On the other hand, if $p \in LP(LP(X))$, the lemma from Theorem 4.6 asserts that $p \in LP(X)$, and we are done again. $\square$

Our next goal is to prove that $\mathbb{Q}$ is dense in $\mathbb{R}$. Just to make sense of that statement, we need to decide how to think of $\mathbb{Q}$ as a subset of $\mathbb{R}$. For every rational number $q \in \mathbb{Q}$, define the corresponding real number as the Dedekind cut

$$i(q) = \{x \in \mathbb{Q} \mid x < q\}$$

For example, $\mathbf{0} = i(0)$. It can be verified that this gives a well-defined injective function $i : \mathbb{Q} \to \mathbb{R}$. We identify $\mathbb{Q}$ with its image $i(\mathbb{Q}) \subset \mathbb{R}$ so that the rational numbers $\mathbb{Q}$ are a subset of the real numbers $\mathbb{R}$. (Similarly, $\mathbb{N}$ and $\mathbb{Z}$ can be understood as subsets of $\mathbb{R}$.)

[2] We may use this lemma since it does not depend on this result, Definition 6.8, or Lemma 6.9.

Lemma 6.10. *Given $A, B \in \mathbb{R}$ with $A < B$, there exists $p \in \mathbb{Q}$ such that $A < i(p) < B$.*

Proof. Since $A < B$, Definition 6.4 tells us that $A \subsetneq B$. Thus, by Definition 1.3, there exists a point q such that $q \in B$ and $q \notin A$. Since $q \in B$ where B is a Dedekind cut, we have by Definition 6.1 that there exists a point $p \in B$ with $p > q$. Additionally, since $q \notin A$ implies that q is an upper bound of A by Lemma 6.2, we know by Definition 5.6 that $x \leq q$ for all $x \in A$. It follows since $q < p$ that $x \leq p$ for all $x \in A$, meaning by Definition 5.6 and Lemma 6.2 that $p \notin A$. Having established that $p, q \in B$, $p, q \notin A$, and $q < p$, we are now ready to prove that $A < i(p) < B$. Definition 6.4 tells us that we may do so by showing that $A \subsetneq i(p)$ and $i(p) \subsetneq B$. We will take this one argument at a time.

To show that $A \subsetneq i(p)$, Definition 1.3 tells us that it will suffice to verify that every element of A is an element of $i(p)$ and that there exists an element of $i(p)$ that is not an element of A. We treat the former statement first. As previously mentioned, $x \leq p$ for all $x \in A$. This combined with the fact that $p \notin A$ implies that $x < p$ for all $x \in A$. Thus, by the definition of $i(p)$, $x \in i(p)$ for all $x \in A$, as desired. As to the latter statement, since $q < p$, we have by the definition of $i(p)$ that $q \in i(p)$. However, we also know that $q \notin A$, as desired.

To show that $i(p) \subsetneq B$, we must verify symmetric arguments to before. For the former statement, let r be an arbitrary element of $i(p)$. Then by the definition of $i(p)$, $r < p$. Since $p \in B$ and $r \in \mathbb{Q}$ satisfy $r < p$, we have by Definition 6.1 that $r \in B$, as desired. As to the latter statement, p is clearly an element of B that is not an element of $i(p)$, as desired. □

1/19: **Theorem 6.11.** *$i(\mathbb{Q})$ is dense in $\mathbb{R}$.*

Proof. To prove that $i(\mathbb{Q})$ is dense in $\mathbb{R}$, Definition 6.8 tells us that it will suffice to show the every point $X \in \mathbb{R}$ is a limit point of $i(\mathbb{Q})$. Let X be an arbitrary element of $\mathbb{R}$. To show that $X \in LP(i(\mathbb{Q}))$, Definition 3.13 tells us that it will suffice to verify that for every region $\underline{AB}$ with $X \in \underline{AB}$, we have $\underline{AB} \cap (i(\mathbb{Q}) \setminus \{X\}) \neq \emptyset$. Let $\underline{AB}$ be an arbitrary region with $X \in \underline{AB}$. It follows by Definitions 3.10 and 3.6 that $A < X < B$. Thus, by Lemma 6.10, there exists $p \in \mathbb{Q}$ such that $A < i(p) < X < B$. By Definitions 3.6 and 3.10, $i(p) \in \underline{AB}$. By Definition 1.18, $i(p) \in i(\mathbb{Q})$. By Exercise 6.5, $i(p) < X$ implies that $i(p) \neq X$. Combining the last three results with Definitions 1.11 and 1.6, we have that $i(p) \in \underline{AB} \cap (i(\mathbb{Q}) \setminus \{X\})$, as desired. □

Corollary 6.12 (The Archimedean Property)**.** *Let $A \in \mathbb{R}$ be a positive real number. Then there exist nonzero natural numbers $n, m \in \mathbb{N}$ such that $i(\frac{1}{n}) < A < i(m)$.*

Proof. We will first prove that there exists a nonzero natural number n such that $i(\frac{1}{n}) < A$. We will then prove that there exists a nonzero natural number m such that $A < i(m)$. Let's begin.

Since $A \in \mathbb{R}$ is positive, we know that $0 < A$. Thus, by Lemma 6.10, there exists $\frac{p}{n} \in \mathbb{Q}$ such that $0 < i(\frac{p}{n}) < A$. As permitted by Exercise 3.9b, we choose $\frac{p}{n} \in \left[\frac{p}{n}\right]$ to be an object such that $0 < n$ (this also means that $n \in \mathbb{N}$). Consequently, by Scripts 2 and 3, we know that $0 < \frac{1}{n} \leq \frac{p}{n}$. It follows that $i(\frac{1}{n}) \leq i(\frac{p}{n})$ since $x \in i(\frac{1}{n})$ implies $x < \frac{1}{n} \leq \frac{p}{n}$ implies $x \in i(\frac{p}{n})$, implies $i(\frac{1}{n}) \subset i(\frac{p}{n})$. Therefore, $i(\frac{1}{n}) \leq i(\frac{p}{n}) < A$, as desired.

By Exercise 6.5, Axiom 3, and Definition 3.3, there exists a point $B \in \mathbb{R}$ such that $A < B$. It follows by Lemma 6.10 that there exists $\frac{m}{q} \in \mathbb{Q}$ such that $A < i(\frac{m}{q}) < B$. As before, let $\frac{m}{q}$ be an object such that $0 < q$. Consequently, by Scripts 2 and 3, we know that $0 < \frac{m}{q} \leq m$. Once again, for the same reasons as before, $i(\frac{m}{q}) \leq i(m)$. Therefore, $A < i(\frac{m}{q}) \leq i(m)$, as desired. □

Corollary 6.13. *$i(\mathbb{N})$ is an unbounded subset of $\mathbb{R}$.*

Proof. Suppose for the sake of contradiction that $i(\mathbb{N})$ is bounded above. Then by Definition 5.6, there exists a point $A \in \mathbb{R}$ such that $i(n) \leq A$ for all $n \in \mathbb{N}$. Note that A is a positive real number since $i(0) < i(0) \leq A$. But by Corollary 6.12, $A < i(n)$ for some $n \in \mathbb{N}$, a contradiction. □

1/21: **Corollary 6.14.** *If $A \in \mathbb{R}$ is a real number, then there is an integer n such that $i(n-1) \leq A < i(n)$.*

Proof. Let X be be the set of all integers z such that $i(z) \leq A$. Symbolically,

$$X = \{z \mid z \in \mathbb{Z} \text{ and } i(z) \leq A\}$$

Since $A \neq \emptyset$ by Definition 6.1, there exists a point $\frac{p}{q} \in \mathbb{Q}$ such that $\frac{p}{q} \in A$. As in Corollary 6.12, we let $q > 0$. It follows by Scripts 2 and 3 that if $p \geq 0$, then $0 \leq \frac{p}{q}$, i.e.[3], $i(0) \leq A$ and if $p < 0$, then $p \leq \frac{p}{q}$, i.e., $i(p) \leq A$. Thus, in either case, X is nonempty.

Now there exists a nonzero natural number m such that $A < i(m)$ (if $A \leq i(0)$, then $A < i(1)$; if $A > 0$, then apply Corollary 6.12). Let $f : X \to \mathbb{N}$ be defined by the rule

$$f(x) = m - x$$

By Script 1, f is an injective function, $f(X) \subset \mathbb{N}$, and $f(X)$ is nonempty (since X is nonempty). Thus, by the well-ordering principle (Additional Exercise 0.1), there is a least element, which we shall call y, in $f(X)$. Since f is injective, there exists exactly one object $n-1 \in X$ such that $f(n-1) = y$.

By the definition of X, $i(n-1) \leq A$. To prove that $A < i(n)$, suppose for the sake of contradiction that $i(n) \leq A$. This coupled with the fact that $n \in \mathbb{Z}$ implies that $n \in X$. Thus, $f(n) \in f(X)$. But $f(n) = m - n < m - n + 1 = m - (n-1) = f(n-1)$, contradicting the fact that $f(n-1)$ is the least element of $f(X)$. ☐

1/26: **Axiom 1.** *The continuum contains a countable dense subset.*

Definition 6.15. Let X and Y be sets with orderings $<_X$ an $<_Y$, respectively. A function $f : X \to Y$ is **order-preserving** if for all $r, s \in X$,

$$r <_X s \Longrightarrow f(r) <_Y f(s)$$

Note that the function $i : \mathbb{Q} \to \mathbb{R}$ discussed above is order-preserving.

Exercise 6.16. Let C satisfy Axioms 1-5. Let $K \subset C$ be a countable dense subset of C. Construct an order-preserving bijection $f : \mathbb{Q} \to K$.

Lemma.

a) *K satisfies Axiom 3.*

b) (Density Lemma) *For all $x, y \in K$, if $x < y$, then there exists a point $z \in K$ such that z is between x and y.*

Proof of a. To prove that K satisfies Axiom 3, we must verify that K has neither a first nor a last point. We will address the first point question first. Suppose for the sake of contradiction that K has a first point x. Then by Definition 3.3, $x \leq y$ for all $y \in K$. However, since C satisfies Axiom 3, there exists an object $a \in C$ such that $a < x$. Now consider the region $\underline{ax}$. We have by Corollary 5.3 that there exists a point $p \in \underline{ax}$. Additionally, we have by Script 3 that $\underline{ax} \cap K = \emptyset$. Thus, $\underline{ax} \cap (K \setminus \{p\}) = \emptyset$, implying by Definition 3.13 that $p \notin LP(K)$. But since $p \in C$ and $p \notin LP(K)$, we have by Definition 6.8 that K is not dense in C, a contradiction.

The proof is symmetric for last points. ☐

Proof of b. Suppose for the sake of contradiction that that there exist $x, y \in K$ with $x < y$ such that no point $z \in K$ is between x and y. By Theorem 5.2, there exists $p \in C$ such that p is between x and y. Consequently, by Definition 3.10, $p \in \underline{xy}$. Additionally, we have by Script 3 that $\underline{xy} \cap K = \emptyset$. It follows that $\underline{xy} \cap (K \setminus \{p\}) = \emptyset$, implying by Definition 3.13 that $p \notin LP(K)$. But since $p \in C$ and $p \notin LP(K)$, we have by Definition 6.8 that K is not dense in C, a contradiction. ☐

[3] For the same reasons as in Corollary 6.12.

Proof of Exercise 6.16. By Theorem 2.11, $\mathbb{Q}$ is countable, implying by Definition 1.35 that there exists a bijection $g : \mathbb{N} \to \mathbb{Q}$. The existence of this bijection means that we can refer to an arbitrary element q of $\mathbb{Q}$ by the number n for which $g(n) = q$; in another notation, we can refer to q as q_n. Thus, since every element of $\mathbb{Q}$ can be written as q_n for some $n \in \mathbb{N}$, we can write $\mathbb{Q} = \{q_1, q_2, \dots\}$. Similarly, we can express K as $K = \{k_1, k_2, \dots\}$. We will use this method of referring to the elements of $\mathbb{Q}$ to construct f.

We define f recursively with strong induction. For the base case q_1, we define $f(q_1) = k_1$. Now suppose inductively that we have defined $f(q_1), f(q_2), \dots, f(q_n)$; we now seek to define $f(q_{n+1})$. By Theorem 3.5, the symbols $a_1, \dots, a_{n+1}$ can be assigned to $q_1, \dots, q_{n+1}$ so that $a_1 <_{\mathbb{Q}} a_2 <_{\mathbb{Q}} \cdots <_{\mathbb{Q}} a_{n+1}$. We divide into three cases ($q_{n+1} = a_1$, $q_{n+1} = a_{n+1}$, and $q_{n+1} = a_i$ where $1 < i < n+1$). First, suppose that $q_{n+1} = a_1$. By the inductive hypothesis, $f(a_2), f(a_3), \dots, f(a_{n+1})$ are defined elements of K. At this point, define the set $X = \{k \in K \mid k <_K f(a_2)\}$. It follows by Lemma (a) that this set is nonempty. Thus, by the well-ordering principle, there exists a $k_i \in X$ such that $i \leq j$ for all $k_j \in X$. We let $f(q_{n+1}) = k_i$. The second case is symmetric to the first. Third, suppose that $q_{n+1} = a_i$ where $1 < i < n+1$. By the inductive hypothesis, $f(a_1), \dots, f(a_{i-1}), f(a_{i+1}), \dots, f(a_{n+1})$ are defined elements of K. At this point, define the set $X = \{k \in K \mid f(a_{i-1}) <_K k <_K f(a_{i+1})\}$. It follows by Lemma (b) that this set is nonempty. Thus, by the well-ordering principle, there exists a $k_i \in X$ such that $i \leq j$ for all $k_j \in X$. We let $f(q_{n+1}) = k_i$.

To prove that f is a function, Definition 1.16 tells us that it will suffice to show that for all $q \in \mathbb{Q}$, there exists a unique $k \in K$ such that $f(q) = k$. First, we will prove that for all $q \in \mathbb{Q}$, there exists *some* $k \in K$ such that $f(q) = k$. Let q_i be an arbitrary element of $\mathbb{Q}$. Then $i \in \mathbb{N}$, and by the principle of strong mathematical induction (Additional Exercise 0.2b), $f(q_i)$ is assigned to an element of k. As to proving the uniqueness of the k to which q_i is defined, each q is assigned once, in one of three mutually exclusive cases, to an unambiguously defined (as guaranteed by the well-ordering principle) element of K.

To prove that f is order-preserving, we will first verify the following claim (which we will refer to as Lemma (c) for future reference): Consider the set $\{q_1, \dots, q_n\} \subset \mathbb{Q}$; if the symbols $a_1, \dots, a_n$ are assigned to $q_1, \dots, q_n$ such that $a_1 <_{\mathbb{Q}} a_2 <_{\mathbb{Q}} \cdots <_{\mathbb{Q}} a_n$, then $f(a_1) <_K f(a_2) <_K \cdots <_K f(a_n)$. We will then use this result to prove that f is order-preserving for any two arbitrary elements $q_i, q_j \in \mathbb{Q}$. Let's begin.

To verify the above claim, we induct on n. The base case $n = 1$ is vacuously true. Now suppose inductively that we have proven the claim for n; we now seek to prove it for $n+1$. By Theorem 3.5, the symbols $a_1, \dots, a_{n+1}$ can be assigned to $q_1, \dots, q_{n+1}$ so that $a_1 <_{\mathbb{Q}} a_2 <_{\mathbb{Q}} \cdots <_{\mathbb{Q}} a_{n+1}$. We divide into three cases ($q_{n+1} = a_1$, $q_{n+1} = a_{n+1}$, and $q_{n+1} = a_i$ where $1 < i < n+1$). First, suppose that $q_{n+1} = a_1$. By the definition of f, $f(q_{n+1}) \in \{k \in K \mid k <_K f(a_2)\}$, meaning that $f(q_{n+1}) = f(a_1) <_K f(a_2)$. Additionally, by the inductive hypothesis, we know that $f(a_2) <_K f(a_3) <_K \cdots <_K f(a_{n+1})$ (since $a_2, \dots, a_{n+1}$ correspond to $q_1, \dots, q_n$). Together, these two results imply that $f(a_1) <_K f(a_2) <_K \cdots <_K f(a_{n+1})$. The proof of the second case is symmetric to that of the first. Third, suppose that $q_{n+1} = a_i$ where $1 < i < n+1$. By the definition of f, $f(q_{n+1}) \in \{k \in K \mid f(a_{i-1}) <_K k <_K f(a_{i+1})\}$, meaning that $f(a_{i-1}) <_K f(q_{n+1}) = f(a_i) <_K f(a_{i+1})$. Additionally, by the inductive hypothesis, we know that $f(a_1) <_K \cdots <_K f(a_{i-1}) <_K f(a_{i+1}) <_K \cdots <_K f(a_{n+1})$ (for an analogous reason to before). These two results imply that $f(a_1) <_K f(a_2) <_K \cdots <_K f(a_{n+1})$.

We are now ready to actually prove that f is order-preserving. To do so, Definition 6.15 tells us that it will suffice to show that for all $q_i, q_j \in \mathbb{Q}$, $q_i <_{\mathbb{Q}} q_j$ implies $f(q_i) <_K f(q_j)$. Let q_i, q_j be arbitrary elements of $\mathbb{Q}$ such that $q_i <_{\mathbb{Q}} q_j$. Since $q_i <_{\mathbb{Q}} q_j$, $q_i \neq q_j$, implying that $i \neq j$. We divide into two cases ($i < j$ and $i > j$). Suppose first that $i < j$. By Theorem 3.5, the symbols $a_1, \dots, a_j$ can be assigned to $q_1, \dots, q_j$ so that $a_1 <_{\mathbb{Q}} a_2 <_{\mathbb{Q}} \cdots <_{\mathbb{Q}} a_j$. Let $q_j = a_l$. Since $q_i <_{\mathbb{Q}} q_j$, we know that $q_i = a_m$ where $m < l$. Additionally, by Lemma (c), we know that $f(a_1) <_K f(a_2) <_K \cdots <_K f(a_j)$. It follows that $f(a_m) <_K f(a_l)$, implying that $f(q_i) <_K f(q_j)$, as desired. The proof is symmetric in the other case.

To prove that f is bijective, Definition 1.20 tells us that it will suffice to show that f is injective and surjective.

To show that f is injective, Definition 1.20 tells us that it will suffice to demonstrate that $q_i \neq q_j$ implies $f(q_i) \neq f(q_j)$. WLOG let $q_i <_{\mathbb{Q}} q_j$. Then since f is order-preserving, Definition 6.15 implies that $f(q_i) <_K f(q_j)$. It follows that $f(q_i) \neq f(q_j)$, as desired.

We are now ready to actually show that f is surjective. To do so, Definition 1.20 tells us that it will suffice to demonstrate that for all $k_n \in K$, there exists a $q_i \in \mathbb{Q}$ such that $f(q_i) = k_n$. To do this, we induct on n. For the base case $n = 1$, it follows from the definition of f that $f(q_1) = k_1$. Now suppose inductively that for each $k_1, \dots, k_n$, there exists a $q_i \in \mathbb{Q}$ such that $f(q_i) = k_n$; we now seek to prove the claim for $n+1$.

By Theorem 3.5, the symbols $b_1, \dots, b_{n+1}$ can be assigned to $k_1, \dots, k_{n+1}$ so that $b_1 <_K b_2 <_K \cdots <_K b_{n+1}$. We divide into three cases ($k_{n+1} = b_1$, $k_{n+1} = b_{n+1}$, and $k_{n+1} = b_i$ where $1 < i < n+1$). First, suppose that $k_{n+1} = b_1$. By the inductive hypothesis, $b_2 = f(q_i) <_K b_3 = f(q_j) <_K \cdots <_K b_{n+1} = f(q_l)$. It follows by Definition 6.15 that $q_i <_{\mathbb{Q}} q_j <_{\mathbb{Q}} \cdots <_{\mathbb{Q}} q_l$. At this point, define the set $X = \{q \in \mathbb{Q} \mid q <_{\mathbb{Q}} q_i\}$. It follows from Exercise 3.9d that this set is nonempty. Thus, by the well-ordering principle, there exists a $q_m \in X$ such that $m \leq m'$ for all $q_{m'} \in X$. By the definition of f, $f(q_m) = k_{n+1}$. The proof of the second case is symmetric to that of the first. Third, suppose that $k_{n+1} = b_i$ where $1 < i < n+1$. By the inductive hypothesis, $b_2 = f(q_j) <_K \cdots <_K b_{i-1} = f(q_{j'}) <_K b_{i+1} = f(q_l) <_K \cdots <_K b_{n+1} = f(q_{l'})$. It follows by Definition 6.15 that $q_j <_{\mathbb{Q}} \cdots <_{\mathbb{Q}} q_{j'} <_{\mathbb{Q}} q_l <_{\mathbb{Q}} \cdots <_{\mathbb{Q}} q_{l'}$. At this point, define the set $X = \{q \in \mathbb{Q} \mid q_{j'} <_{\mathbb{Q}} q <_{\mathbb{Q}} q_l\}$. It follows from Additional Exercise 3.1 that this set is nonempty. Thus, by the well-ordering principle, there exists a $q_m \in X$ such that $m \leq m'$ for all $q_{m'} \in X$. By the definition of f, $f(q_m) = k_{n+1}$. □

Exercise 6.17. Let $f : \mathbb{Q} \to K$ be an order-preserving bijection, as found in Exercise 6.16. Let $A \in \mathbb{R}$. Then $A \subset \mathbb{Q}$ and so $f(A) \subset K \subset C$. Define $F : \mathbb{R} \to C$ by

$$F(A) = \sup f(A)$$

1. Show $\sup f(A)$ exists, so F is well-defined.

2. Show F is injective and order-preserving.

Proof of 1. To prove that $\sup f(A)$ exists, Theorem 5.17 tells us that it will suffice to show that $f(A)$ is nonempty and bounded above. To show that $f(A)$ is nonempty, Definition 1.8 tells us that it will suffice to find an element of $f(A)$. By Definition 6.1, $A \neq \emptyset$. Thus, by Definition 1.8, there exists an object $x \in A$. It follows by Definition 1.18 that $f(x) \in f(A)$, as desired. To show that $f(A)$ is bounded above, Definition 5.6 tells us that it will suffice to find an element of K such that $f(x) \geq_C f(a)$ for all $f(a) \in f(A)$. By Definition 6.1, $A \neq \mathbb{Q}$ and $A \subset \mathbb{Q}$. Thus, by Definition 1.2, there exists an object $x \in \mathbb{Q}$ such that $x \notin A$. It follows from the latter condition by Lemma 6.2 that x is an upper bound for A. Thus, by Definition 5.6, $x \geq a$ for all $a \in A$. Consequently, by Definition 6.15, $f(x)$ is an element of K such that $f(x) \geq_C f(a)$ for all $f(a) \in f(A)$, as desired. □

Proof of 2. To prove that F is order-preserving, Definition 6.15 tells us that it will suffice to show that for all $A, B \in \mathbb{R}$, $A <_{\mathbb{R}} B$ implies $F(A) <_C F(B)$. Let A, B be two arbitrary elements of $\mathbb{R}$ satisfying $A <_{\mathbb{R}} B$. Then by Definitions 6.4 and 1.3, there exists a point $x \in B$ such that $x \notin A$. It follows from the latter condition by Lemma 6.2 and Definition 5.6 that $x \geq a$ for all $a \in A$. Thus, by Definition 6.15, $f(x) \geq_C f(a)$ for all $f(a) \in f(A)$. Consequently, by Definition 5.7, $\sup f(A) \leq_C f(x)$. Additionally, by Definition 6.1, there exists a point $y \in B$ such that $y > x$. Thus, by Definition 6.15, we have that $f(y) >_C f(x)$. It follows by Definitions 5.6 and 5.7 that $f(y) \leq_C \sup f(B)$. Combining two results, we therefore have that $\sup f(A) \leq_C f(x) <_C f(y) \leq_C \sup f(B)$, meaning that $F(A) = \sup f(A) <_C \sup f(B) = F(B)$, as desired.

To prove that F is injective, Definition 1.20 tells us that it will suffice to show that if $A \neq B$, then $F(A) \neq F(B)$. Let A, B be two distinct real numbers. Then by Exercise 6.5, $A < B$ or $B < A$. We now divide into two cases. Suppose first that $A < B$. Then $F(A) < F(B)$ by Definition 6.15 (which we have just proven applies to F). This implies by Definition 3.1 that $F(A) \neq F(B)$, as desired. The proof is symmetric in the other case. □

Theorem 6.18. *Suppose that C is a continuum satisfying Axioms 1-5. Then C is isomorphic to the real numbers $\mathbb{R}$; i.e., there is an order-preserving bijection $F : \mathbb{R} \to C$.*

Lemma. *Let K be a dense subset of C. For all $x, y \in C$, if $x < y$, then there exists a point $z \in K$ such that z is between x and y.*

Proof. Suppose for the sake of contradiction that there exist two points $x, y \in C$ with $x < y$ such that no point $z \in K$ is between x and y. By Corollary 5.3, the region $\underline{xy}$ is infinite. Thus, we can pick a point $p \in \underline{xy}$. Additionally, by Definition 1.6, we have that $\underline{xy} \cap K = \emptyset$. Thus, $\underline{xy} \cap (K \setminus \{p\}) = \emptyset$, implying by Definition 3.13 that $p \notin LP(K)$. But since $p \in C$ and $p \notin LP(K)$, we have by Definition 6.8 that K is not dense in C, a contradiction. □

Proof of Theorem 6.18. By Axiom 1, C contains a countable dense subset K. By Exercise 6.16, there exists an order-preserving bijection $f : \mathbb{Q} \to K$. By Exercise 6.17, there exists an order-preserving injection $F : \mathbb{R} \to C$. To prove that there is an order-preserving bijection $F : \mathbb{R} \to C$, all that is left to do is to demonstrate that F (as defined in Exercise 6.17) is surjective.

To do this, Definition 1.20 tells us that it will suffice to show that for all $X \in C$, there exists an object $A \in \mathbb{R}$ such that $F(A) = X$. Put more simply, we must find a Dedekind cut A such that $\sup f(A) = X$ for every $X \in C$. To do this, we will begin by constructing the set $S = \{k \in K \mid k < X\}$. We will then verify that the preimage $f^{-1}(S)$ is a Dedekind cut. Lastly, we will verify that $\sup f(f^{-1}(S)) = X$. Let's begin.

Let X be an arbitrary element of C. Define S as above. To verify that $f^{-1}(S)$ is a Dedekind cut, Definition 6.1 tells us that it will suffice to confirm that $f^{-1}(S) \neq \emptyset$; $f^{-1}(S) \neq \mathbb{Q}$; if $r \in f^{-1}(S)$ and $s \in \mathbb{Q}$ satisfy $s < r$, then $s \in f^{-1}(S)$; and if $r \in f^{-1}(S)$, then there is some $s \in f^{-1}(S)$ with $s > r$. We will take this one claim at a time.

To confirm that $f^{-1}(S) \neq \emptyset$, Definition 1.8 tells us that it will suffice to find an element of $f^{-1}(S)$. By Axiom 3 and Definition 3.3, there exists some point $Y \in C$ such that $Y < X$. Consequently, by the lemma and Definition 3.6, there exists a point $f(p) \in K$[4] such that $Y < f(p) < X$. It follows by the definition of S that $f(p) \in S$. Therefore, by Definition 1.18, $p \in f^{-1}(S)$, as desired.

To confirm that $f^{-1}(S) \neq \mathbb{Q}$, Definition 1.2 tells us that it will suffice to find an element of $\mathbb{Q}$ that is not an element of $f^{-1}(S)$. By Axiom 3 and Definition 3.3, there exists some point $Y \in C$ such that $X < Y$. Consequently, by the lemma and Definition 3.6, there exists a point $f(p) \in K$ such that $X < f(p) < Y$. It follows by the definition of S that $f(p) \notin S$. Therefore, by Definition 6.18, $p \in \mathbb{Q}$ but $p \notin f^{-1}(S)$, as desired.

To confirm that if $r \in f^{-1}(S)$ and $s \in \mathbb{Q}$ satisfy $s < r$, then $s \in f^{-1}(S)$, we let $r \in f^{-1}(S)$ and $s \in \mathbb{Q}$ be arbitrary elements of their respective sets that satisfy $s < r$ and seek to verify that $s \in f^{-1}(S)$. By Definition 1.18, the fact that $r \in f^{-1}(S)$ implies that $f(r) \in S$. Thus, by the definition of S, $f(r) < X$. Additionally, by the definition of f and Definition 6.15, $f(s) \in K$ and $f(s) < f(r)$, respectively. Since $f(s) < f(r)$ and $f(r) < X$, transitivity implies that $f(s) < X$. This combined with the previously established fact that $f(s) \in K$ implies that $f(s) \in S$. Therefore, by Definition 1.18, $s \in f^{-1}(S)$, as desired.

To confirm that if $r \in f^{-1}(S)$, then there is some $s \in f^{-1}(S)$ with $s > r$, we let $r \in f^{-1}(S)$ and seek to find such an s. As before, $r \in f^{-1}(S)$ implies that $f(r) \in S$. Thus, by the definition of S, $f(r) < X$. It follows by the lemma and Definition 3.6 that there exists a point $f(s) \in K$ such that $f(r) < f(s) < X$. Consequently, by the definition of S, we have that $f(s) \in S$. Therefore, by Definitions 1.18 and 6.15, $s \in f^{-1}(S)$ and $r < s$, respectively, as desired.

Since f is bijective, Script 1 asserts that $f(f^{-1}(S)) = S$. Thus, $\sup f(f^{-1}(S)) = \sup S$. To verify that $\sup S = X$, Definition 5.7 tells us that it will suffice to confirm that X is an upper bound of S and if U is an upper bound of S, $X \leq U$. To confirm the former statement, Definition 5.6 tells us that it will suffice to show that $k \leq X$ for all $k \in S$. But by the definition of S, this is true. To confirm the latter statement, suppose for the sake of contradiction that there exists an upper bound U of S such that $U < X$. Since $U < X$, the lemma and Definition 3.6 imply that there exists a point $Z \in K$ such that $U < Z < X$. It follows by the definition of S that $Z \in S$. Since there exists an element of S greater than U, Definition 5.6 asserts that U is not an upper bound of S, a contradiction. □

6.2 Discussion

1/12:

- Upper limit at signing up for 4-5 across the script.
- Lemma 6.2 is probably more straightforward using a contradiction argument.
- Briefly restate the algebra of Exercise 4.24 in Exercise 6.3c.

1/14:

- Turning in Script 5 journals is optional — it will boost your grade a bit if you do.
  - Your journal grade will be whichever is higher: the average of all your journal grades with and without Script 5.

[4]Note that we know that the element of K (the existence of which is implied by the lemma) can be written in the form $f(p)$ because f is bijective.

  - Script 5 will probably be due Wednesday, 1/20.

- In Lemma 6.6, do we need to prove that the union of arbitrarily many Dedekind cuts is, itself, a Dedekind cut? Yes.

1/18:
- Is there a way to prove something else besides A is not open in Exercise 6.7?
  - This is probably it as far as proving that continuua are connected.
  - It may not be possible to prove that *any* of the statements are wrong, but he's not sure.
- Is Lemma 6.9 used in the proofs of any subsequent results, or is it just a less important result (hence the lemma designation)?
  - We can think of it as an alternate definition for density — we could prove Definition 6.8 from it.
- Is my handwavey use of Scripts 2 and 3 ok in Corollary 6.12?
  - I'm fine.
- Is there a simpler way to prove Corollaries 6.12 and 6.14?
  - hi
- Is the math REU still running this summer?
  - He's not sure; UChicago's may not be NSF approved, hence why its not on the website rn.
- What other summer opportunities would you recommend for a student at my level?
  - He did an REU at UWisconsin when he was an undergrad.
  - Sounds like its pretty much just REUs for undergrads.
  - I could ask around to see if anyone is a Knot Theorist/willing to sponsor me.

1/19:
- Easier Corollary 6.12:
  - Let $B > A$. Then $A < i(\frac{m}{q}) < B$. Then $A < i(m)$.
- Several proofs were given for Corollary 6.14. One other correct one constructed the nonempty, bounded above set of all $i(n)$ less than or equal to A and considered its supremum.

1/21:
- Now graded a bit more critically on presentations.
  - Write big, talk loudly, don't talk to the blackboard.
- My original proof of Corollary 6.14 is incorrect because I can't split into cases the way I did (*longer expo*).
  - Instead, use Seb's approach.

1/26:
- Stray thoughts on Exercise 6.16:
  - Any property we can prove for $\mathbb{Q}$ (e.g., betweenness, Axioms 1-3, etc.) we should be able to prove for K.
    * Many of these follow from $\mathbb{Q}$'s density! This is how we can make use of this condition.
  - We think of 0 as being somehow the "midpoint" of $\mathbb{Q}$. But since $\mathbb{Q}$ diverges in both directions, it doesn't really have a midpoint; we just assert this rather arbitrary structure on a more foundational algebraic construct.
    * The same would hold for K. Thus, we can choose an arbitrary point $x \in K$ and let it be the "midpoint," i.e., let $f(0) = x$.
  - Can we induct on the elements of $\mathbb{Q}$? Since there exists a bijection $\mathbb{Q} \to \mathbb{N}$.

- We can construct an order preserving bijection between any finite subsets of $\mathbb{Q}$ and K with equal cardinality.
- $f : \mathbb{Q} \to K$, $g : \mathbb{N} \to \mathbb{Q}$, $h : \mathbb{N} \to K$. If $g(n) < g(n')$, then $h(n) < h(n')$.
- Let $h(n) < h(n')$. WLOG let $n < n'$, too. Now consider $N = \{n \in \mathbb{N} \mid n \leq n'\}$. This is a finite set. Now create a new set $g(N)$. There will be an order-preserving bijection $\tilde{f} : h(N) \to g(N)$.
- Let $g : \mathbb{N} \to \mathbb{Q}$ be a bijection (we know one exists by countability). We presently seek to define $h : \mathbb{N} \to K$ recursively. Let x_1 be an arbitrary element of K (Axiom 1). We define $h(1) = x_1$. Now suppose inductively that we have defined $h(n)$. We now seek to define $h(n+1)$. Consider the set $A = \{g(m) \mid m \leq n+1\}$. By Theorem 3.5, we can assign the symbols $a_1, \dots, a_{n+1}$ to each point of A so that $a_1 < a_2 < \cdots < a_{n+1}$. We know that $g(n+1) = a_i$ for some $i \in [n+1]$. We divide into three cases ($g(n+1) = b_1$, $g(n+1) = b_{n+1}$, and $g(n+1) = b_i$ where $1 < i < n+1$). First, suppose that $g(n+1) = b_1$. By the inductive hypothesis, $h(g^{-1}(b_2)) \in K$. By Axiom 3, $h(g^{-1}(b_2))$ is not the first point of K. Thus, there exists an $x \in K$ such that $x < h(g^{-1}(b_2))$. Consequently, let $h(n+1) = x$. The proof of the second case is symmetric to that of the first. Third, suppose that $g(n+1) = b_i$ where $1 < i < n+1$. By the inductive hypothesis, $h(g^{-1}(b_{i-1})), h(g^{-1}(b_{i+1})) \in K$. Thus, there exists an $x \in K$ such that $h(b_{i-1}) < x < h(b_{i+1})$. Consequently, let $h(n+1) = x$.
- We define $f : \mathbb{Q} \to K$ by $f(p) = h(g^{-1}(p))$.
- Function diagram: The characteristic of an order preserving bijection is no intersections between lines connecting elements of different sets.

- Do we need to have subscripts on our orderings? Yes.
- The canonical way of doing Exercise 6.16 is with the **back and forth method**.
  - Because both are countable, $\mathbb{Q} = \{q_1, q_2, \dots\}$. Likewise, $K = \{k_1, k_2, \dots\}$.
  - To create the bijection, we have two repeating steps.
    1. Let i be the smallest index such that q_i has not been paired. Let j be an index such that k_j hasn't been paired, and assigning $f(q_i) = k_j$ preserves ordering (we have to prove that such a j exists). To prove this, we know that we can order the elements of $\mathbb{Q}$ that have already been paired. We can also order the elements of K that have already been paired. Case 1: q_i is between some preexisting q's. Then there exists some k_j between. Case 2: $q_i < \cdots < q_n$ implies there exists some k_j less than all other k so far. Case 3: q_i is a last element; symmetric to Case 2.
    2. Smallest j, smallest i such that order is preserved. Then we let $f(q_i) = k_j$.
    3. Repeat.
  - Injectivity: Suppose $f(q_i) = f(q_j)$. Each q_k is assigned to a unique k_k, so if they're equal, they must have been assigned at the same time. Therefore, $q_i = q_j$.
  - Surjectivity: Let $k_j \in K$. By jth step at most, k_j will be paired.
- Do summer research things every happen with graduate students, or is it just with professors? It pretty much only happens with professors, but DRP could be a good way to get your foot in the door.

Script 7

The Field Axioms

7.1 Journal

1/28: **Definition 7.1.** A **binary operation** on a set X is a function

$$f : X \times X \to X$$

We say that f is **associative** if

$$f(f(x, y), z) = f(x, f(y, z)) \quad \text{for all } x, y, z \in X$$

We say that f is **commutative** if

$$f(x, y) = f(y, x) \quad \text{for all } x, y \in X$$

An **identity element** of a binary operation f is an element $e \in X$ such that

$$f(x, e) = f(e, x) = x \quad \text{for all } x \in X$$

Remark 7.2. Frequently, we denote a binary operation differently. If $* : X \times X \to X$ is the binary operation, we often write $a * b$ in place of $*(a, b)$. We sometimes indicate this same operation by writing $(a, b) \mapsto a * b$.

Exercise 7.3. Rewrite Definition 7.1 using the notation of Remark 7.2.

Answer. A **binary operation** on a set X is a function

$$* : X \times X \to X$$

We say that $*$ is **associative** if

$$(x * y) * z = x * (y * z) \quad \text{for all } x, y, z \in X$$

We say that $*$ is **commutative** if

$$x * y = y * x \quad \text{for all } x, y \in X$$

An **identity element** of a binary operation $*$ is an element $e \in X$ such that

$$x * e = e * x = x \quad \text{for all } x \in X$$

$\square$

Examples 7.4.

1. *The function* $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *which sends a pair of integers* (m, n) *to* $+(m, n) = m + n$ *is a binary operation on the integers, called addition. Addition is associative, commutative, and has identity element 0.*

2. *The maximum of m and n, denoted* $\max(m,n)$*, is an associative and commutative binary operation on* $\mathbb{Z}$*. Is there an identity element for* $\max$*?*

   Proof. Suppose for the sake of contradiction that there exists an identity element e for max. But $\max(e-1,e) = e \neq e-1$, a contradiction. Therefore, no identity element exists for max. □

3. *Let $\wp(Y)$ be the power set of a set Y. Recall that the power set consists of all subsets of Y. Then the intersection of sets, $(A,B) \mapsto A \cap B$, defines an associative and commutative binary operation on $\wp(Y)$. Is there an identity element for $\cap$?*

   Proof. Clearly, $Y \in \wp(Y)$. By Script 1, $Y \cap A = A \cap Y = A$ where $A \subset Y$. Therefore, Y is an identity element for $\cap$. □

Exercise 7.5. Find a binary operation on a set that is not commutative. Find a binary operation on a set that is not associative.

Proof. We will prove that the subtraction operation on the integers ($- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$) is not commutative or associative. To prove that it's not commutative, Definition 7.1 tells us that it will suffice to show that $x - y \neq y - x$ for some $x, y \in \mathbb{Z}$. Since $2 - 1 = 1$ but $1 - 2 = -1$, we can see that $1, 2 \in \mathbb{Z}$ clearly meet this requirement. To prove that it's not associative, Definition 7.1 tells us that it will suffice to show that $(x-y)-z \neq x-(y-z)$ for some $x,y,z \in \mathbb{Z}$. Since $(3-2)-1 = 0$ but $3-(2-1) = 2$, we can see that $1, 2, 3 \in \mathbb{Z}$ clearly meet this requirement. □

Exercise 7.6. Let X be a finite set, and let $Y = \{f : X \to X \mid f \text{ is bijective}\}$. Consider the binary operation of composition of functions, denoted $\circ : Y \times Y \to Y$ and defined by $(f \circ g)(x) = f(g(x))$ as seen in Definition 1.25. Decide whether or not composition is commutative and/or associative and whether or not it has an identity.

Proof. To prove that composition is not commutative, Definition 7.1 tells us that it will suffice to find a finite set X paired with two bijections in Y that do not commute. Let $X = \{1,2,3\}$ and consider the bijections $f : X \to X$ (defined by $f(1) = 2$, $f(2) = 3$, $f(3) = 1$) and $g : X \to X$ (defined by $g(1) = 1$, $g(2) = 3$, $g(3) = 2$). In this case, $f \circ g$ would be defined by $f(g(1)) = 2$, $f(g(2)) = 1$, and $f(g(3)) = 3$, but $g \circ f$ would be defined by $g(f(1)) = 3$, $g(f(2)) = 2$, and $g(f(3)) = 1$.

To prove that composition is associative, Definition 7.1 tells us that it will suffice to show that $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$. We may do this with the following algebra.

$$\begin{aligned}
((f \circ g) \circ h)(x) &= (f \circ g)(h(x)) \\
&= f(g(h(x))) \\
&= f((g \circ h)(x)) \\
&= (f \circ (g \circ h))(x)
\end{aligned}$$

With respect to any finite set X, there will always be a bijection $i : X \to X$ defined by $i(x) = x$. To prove that i is an identity element, Definition 7.1 tells us that it will suffice to show that for all $f \in Y$, $f \circ i = i \circ f = f$. We may do this with the following algebra.

$$\begin{aligned}
(f \circ i)(x) &= f(i(x)) \\
&= f(x) \\
&= i(f(x)) \\
&= (i \circ f)(x)
\end{aligned}$$

□

Theorem 7.7. *Identity elements are unique. That is, suppose that f is a binary operation on a set X that has two identity elements e and e'. Then $e = e'$.*

Proof. Let $f : X \times X \to X$ be a binary operation on a set X with two identity elements e, e'. By Definition 7.1, we know that $f(e, e') = e$ and $f(e, e') = e'$. Since f is a well-defined function by definition, it must be that $e = f(e, e') = e'$. $\square$

Definition 7.8. A **field** is a set F with two binary operations on F called addition, denoted $+$, and multiplication, denoted $\cdot$, satisfying the following **field axioms**:

FA1 (Commutativity of Addition) For all $x, y \in F$, $x + y = y + x$.

FA2 (Associativity of Addition) For all $x, y, z \in F$, $(x + y) + z = x + (y + z)$.

FA3 (Additive Identity) There exists an element $0 \in F$ such that $x + 0 = 0 + x = x$ for all $x \in F$.

FA4 (Additive Inverses) For any $x \in F$, there exists $y \in F$ such that $x + y = y + x = 0$, called an additive inverse of x.

FA5 (Commutativity of Multiplication) For all $x, y \in F$, $x \cdot y = y \cdot x$.

FA6 (Associativity of Multiplication) For all $x, y, z \in F$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

FA7 (Multiplicative Identity) There exists an element $1 \in F$ such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in F$.

FA8 (Multiplicative Inverses) For any $x \in F$ such that $x \neq 0$, there exists $y \in F$ such that $x \cdot y = y \cdot x = 1$, called a multiplicative inverse of x.

FA9 (Distributivity of Multiplication over Addition) For all $x, y, z \in F$, $x \cdot (y + z) = x \cdot y + x \cdot z$.

FA10 (Distinct Additive and Multiplicative Identities) $1 \neq 0$.

Exercise 7.9. Consider the set $\mathbb{F}_2 = \{0, 1\}$, and define binary operations $+$ and $\cdot$ on $\mathbb{F}_2$ by

$$\begin{array}{cccc} 0+0=0 & 0+1=1 & 1+0=1 & 1+1=0 \\ 0\cdot 0=0 & 0\cdot 1=0 & 1\cdot 0=0 & 1\cdot 1=1 \end{array}$$

Show that $\mathbb{F}_2$ is a field.

Proof. To prove that $\mathbb{F}_2$ obeys FA1 from Definition 7.8, it will suffice to show that $0+0 = 0+0$, $0+1 = 1+0$, and $1+1 = 1+1$. The first and third of these are evidently true. For the second, we have $0+1 = 1 = 1+0$, so it is good, too.

To prove that $\mathbb{F}_2$ obeys FA2 from Definition 7.8, the following casework will suffice.

$$\begin{array}{cc} (0+0)+0 = 0 = 0+(0+0) & (0+0)+1 = 1 = 0+(0+1) \\ (0+1)+0 = 1 = 0+(1+0) & (1+0)+0 = 1 = 1+(0+0) \\ (0+1)+1 = 0 = 0+(1+1) & (1+1)+0 = 0 = 1+(1+0) \\ (1+0)+1 = 0 = 1+(0+1) & (1+1)+1 = 1 = 1+(1+1) \end{array}$$

To prove that $\mathbb{F}_2$ obeys FA3 from Definition 7.8, it will suffice to find an element $0 \in \mathbb{F}_2$ such that $x + 0 = 0 + x = x$. Since $0+0 = 0$, $1+0 = 0$, and with commutativity, it is clear that 0 is an additive identity in $\mathbb{F}_2$.

To prove that $\mathbb{F}_2$ obeys FA4 from Definition 7.8, it will suffice to show that for all $x \in \mathbb{F}_2$, there exists a $y \in \mathbb{F}_2$ such that $x + y = y + x = 0$. For 0, this object is 0 (since $0 + 0 = 0 + 0 = 0$), and for 1, this object is 1 (since $1 + 1 = 1 + 1 = 0$).

To prove that $\mathbb{F}_2$ obeys FA5 from Definition 7.8, it will suffice to show that $0 \cdot 0 = 0 \cdot 0$, $0 \cdot 1 = 1 \cdot 0$, and $1 \cdot 1 = 1 \cdot 1$. The first and third of these are evidently true. For the second, we have $0 \cdot 1 = 0 = 1 \cdot 0$, so it is good, too.

To prove that $\mathbb{F}_2$ obeys FA6 from Definition 7.8, the following casework will suffice.

$$\begin{array}{cc} (0\cdot 0)\cdot 0 = 0 = 0\cdot(0\cdot 0) & (0\cdot 0)\cdot 1 = 0 = 0\cdot(0\cdot 1) \\ (0\cdot 1)\cdot 0 = 0 = 0\cdot(1\cdot 0) & (1\cdot 0)\cdot 0 = 0 = 1\cdot(0\cdot 0) \\ (0\cdot 1)\cdot 1 = 0 = 0\cdot(1\cdot 1) & (1\cdot 1)\cdot 0 = 0 = 1\cdot(1\cdot 0) \\ (1\cdot 0)\cdot 1 = 0 = 1\cdot(0\cdot 1) & (1\cdot 1)\cdot 1 = 1 = 1\cdot(1\cdot 1) \end{array}$$

To prove that $\mathbb{F}_2$ obeys FA7 from Definition 7.8, it will suffice to find an element $1 \in \mathbb{F}_2$ such that $x \cdot 1 = 1 \cdot x = x$. Since $0 \cdot 1 = 0$, $1 \cdot 1 = 1$, and with commutativity, it is clear that 1 is a multiplicative identity in $\mathbb{F}_2$.

To prove that $\mathbb{F}_2$ obeys FA8 from Definition 7.8, it will suffice to show that for all $x \in \mathbb{F}_2$ such that $x \neq 0$, there exists a $y \in \mathbb{F}_2$ such that $x \cdot y = y \cdot x = 1$. For 1, this object is 1 (since $1 \cdot 1 = 1 \cdot 1 = 1$).

To prove that $\mathbb{F}_2$ obeys FA9 from Definition 7.8, the following casework will suffice.

$$\begin{array}{ll}
0 \cdot (0+0) = 0 = 0 \cdot 0 + 0 \cdot 0 & 0 \cdot (0+1) = 0 = 0 \cdot 0 + 0 \cdot 1 \\
0 \cdot (1+0) = 0 = 0 \cdot 1 + 0 \cdot 0 & 1 \cdot (0+0) = 0 = 1 \cdot 0 + 1 \cdot 0 \\
0 \cdot (1+1) = 0 = 0 \cdot 1 + 0 \cdot 1 & 1 \cdot (1+0) = 1 = 1 \cdot 1 + 1 \cdot 0 \\
1 \cdot (0+1) = 1 = 1 \cdot 0 + 1 \cdot 1 & 1 \cdot (1+1) = 0 = 1 \cdot 1 + 1 \cdot 1
\end{array}$$

To prove that $\mathbb{F}_2$ obeys FA10 from Definition 7.8, it will suffice to show that $0 \neq 1$. Clearly this is true. □

Theorem 7.10. *Suppose that F is a field. Then additive inverses are unique. This means: Let $x \in F$. If $y, y' \in F$ satisfy $x + y = 0$ and $x + y' = 0$, then $y = y'$.*

Proof. Let $x, y, y' \in F$ be such that $x + y = 0$ and $x + y' = 0$. From Definition 7.8, we have

$$\begin{aligned}
y' + (x+y) &= (y'+x) + y && \text{FA2} \\
y' + 0 &= 0 + y && \text{FA4} \\
y' &= y && \text{FA3}
\end{aligned}$$

□

We usually write $-x$ for the additive inverse of x.

Corollary 7.11. *If $x \in F$, then $-(-x) = x$.*

Proof. Let $x \in F$. Then by consecutive applications of FA4 from Definition 7.8, $-x + (-(-x)) = 0$ and $-x + x = 0$. Therefore, by Theorem 7.10, we have that $-(-x) = x$. □

Theorem 7.12. *Let F be a field, and let $a, b, c \in F$. If $a + b = a + c$, then $b = c$.*

Proof. Let $a, b, c \in F$ be such that $a + b = a + c$. By FA4 from Definition 7.8, there exists $-a \in F$ such that $-a + a = a + (-a) = 0$. Having established that $-a$ exists, we can prove from Definition 7.8 that

$$\begin{aligned}
-a + (a+b) &= -a + (a+c) && \\
(-a+a) + b &= (-a+a) + c && \text{FA2} \\
0 + b &= 0 + c && \text{FA4} \\
b &= c && \text{FA3}
\end{aligned}$$

□

Theorem 7.13. *Let F be a field. If $a \in F$, then $a \cdot 0 = 0$.*

Proof. Let $a \in F$. From Definition 7.8, we have

$$\begin{aligned}
a &= a \cdot 1 && \text{FA7} \\
&= a \cdot (1+0) && \text{FA3} \\
&= a \cdot 1 + a \cdot 0 && \text{FA9} \\
&= a + a \cdot 0 && \text{FA7} \\
0 &= a \cdot 0 && \text{Theorem 7.12}
\end{aligned}$$

□

2/2: **Theorem 7.14.** *Suppose that F is a field. Then multiplicative inverses are unique. This means: Let $x \in F$. If $y, y' \in F$ satisfy $x \cdot y = 1$ and $x \cdot y' = 1$, then $y = y'$.*

Proof. Let $x, y, y' \in F$ be such that $x \cdot y = 1$ and $x \cdot y' = 1$. From Definition 7.8, we have

$$\begin{aligned} (y \cdot x) \cdot y' &= y \cdot (x \cdot y') && \text{FA6} \\ 1 \cdot y' &= y \cdot 1 && \text{FA8} \\ y' &= y && \text{FA7} \end{aligned}$$

□

We usually write x^{-1} or $\frac{1}{x}$ for the multiplicative inverse of x.

Corollary 7.15. *If $x \in F$ and $x \neq 0$, then $(x^{-1})^{-1} = x$.*

Proof. Let $x \in F \setminus \{0\}$. Then by FA8 from Definition 7.8, there exists $x^{-1} \in F$ such that $x \cdot x^{-1} = x^{-1} \cdot x = 1$. It follows from Theorem 7.13 that $x^{-1} \neq 0$ (if $x^{-1} = 0$, then Theorem 7.13 would imply that $x \cdot x^{-1} = 0$, a contradiction). Thus, by FA8 from Definition 7.8 again, there exists $(x^{-1})^{-1} \in F$ such that $x^{-1} \cdot (x^{-1})^{-1} = (x^{-1})^{-1} \cdot x^{-1} = 1$. Having established that $(x^{-1})^{-1}$ exists, $x^{-1} \cdot (x^{-1})^{-1} = 1$, and $x^{-1} \cdot x = 1$, we have by Theorem 7.14 that $(x^{-1})^{-1} = x$. □

Theorem 7.16. *Let F be a field, and let $a, b, c \in F$. If $a \cdot b = a \cdot c$ and $a \neq 0$, then $b = c$.*

Proof. Let $a, b, c \in F$ be such that $a \cdot b = a \cdot c$ and $a \neq 0$. By FA8 from Definition 7.8, there exists $a^{-1} \in F$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. Having established that a^{-1} exists, we can prove from Definition 7.8 that

$$\begin{aligned} a^{-1} \cdot (a \cdot b) &= a^{-1} \cdot (a \cdot c) && \\ (a^{-1} \cdot a) \cdot b &= (a^{-1} \cdot a) \cdot c && \text{FA6} \\ 1 \cdot b &= 1 \cdot c && \text{FA8} \\ b &= c && \text{FA7} \end{aligned}$$

□

Theorem 7.17. *Let F be a field, and let $a, b \in F$. If $a \cdot b = 0$, then $a = 0$ or $b = 0$.*

Proof. Let $a, b \in F$ be such that $a \cdot b = 0$, and suppose for the sake of contradiction that $a \neq 0$ and $b \neq 0$. It follows from the supposition by consecutive applications of FA8 from Definition 7.8 that a^{-1} and b^{-1} exist. Thus, from Definition 7.8, we have

$$\begin{aligned} 1 &= 1 \cdot 1 && \text{FA7} \\ &= (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) && \text{FA8} \\ &= (a \cdot b) \cdot (a^{-1} \cdot b^{-1}) && \text{FA6 and FA7} \\ &= 0 \cdot (a^{-1} \cdot b^{-1}) && \text{Substitution} \\ &= 0 && \text{Theorem 7.13} \end{aligned}$$

But this contradicts FA10 from Definition 7.8. □

Lemma 7.18. *Let F be a field. If $a \in F$, then $-a = (-1)a$.*

Proof. Let $a \in F$. From Definition 7.8, we have

$$\begin{aligned} 0 &= 0 \cdot a && \text{Theorem 7.13} \\ a + (-a) &= (1 + (-1)) \cdot a && \text{FA4} \\ a + (-a) &= 1 \cdot a + (-1) \cdot a && \text{FA9} \\ a + (-a) &= a + (-1)a && \text{FA7} \\ -a &= (-1)a && \text{Theorem 7.12} \end{aligned}$$

□

Lemma 7.19. *Let F be a field. If $a, b \in F$, then $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$.*

Proof. Let $a, b \in F$. From Definition 7.8, we have

$$\begin{aligned} a \cdot (-b) &= a \cdot ((-1) \cdot b) && \text{Lemma 7.18} \\ &= a \cdot (b \cdot (-1)) && \text{FA5} \\ &= (a \cdot b) \cdot (-1) && \text{FA6} \\ &= (-1) \cdot (a \cdot b) && \text{FA5} \\ &\boxed{= -(a \cdot b)} && \text{Lemma 7.18} \\ &= (-1) \cdot (a \cdot b) && \text{Lemma 7.18} \\ &= ((-1) \cdot a) \cdot b && \text{FA6} \\ &\boxed{= (-a) \cdot b} && \text{Lemma 7.18} \end{aligned}$$

□

Lemma 7.20. *Let F be a field. If $a, b \in F$, then $a \cdot b = (-a) \cdot (-b)$.*

Proof. Let $a, b \in F$. Thus, we have

$$\begin{aligned} (-a) \cdot (-b) &= -(-a) \cdot b && \text{Lemma 7.19} \\ &= a \cdot b && \text{Corollary 7.11} \end{aligned}$$

□

Definition 7.21. An **ordered field** is a field F equipped with an ordering $<$ (satisfying Definition 3.1) such that also:

(a) Addition respects the ordering: if $x < y$, then $x + z < y + z$ for all $z \in F$.

(b) Multiplication respects the ordering: if $0 < x$ and $0 < y$, then $0 < x \cdot y$.

Definition 7.22. Suppose F is an ordered field and $x \in F$. If $0 < x$, we say that x is **positive**. If $x < 0$, we say that x is **negative**.

Lemma 7.23. *Let F be an ordered field, and let $x \in F$. If $0 < x$, then $-x < 0$. Similarly, if $x < 0$, then $0 < -x$.*

Proof. Let $x \in F$ be such that $0 < x$. Then by Definition 7.21a, $0 + (-x) < x + (-x)$. Consequently, from Definition 7.8, we have

$$\begin{aligned} -x &< x + (-x) && \text{FA3} \\ -x &< 0 && \text{FA4} \end{aligned}$$

The proof is symmetric if $x < 0$. □

Lemma 7.24. *Let F be an ordered field, and let $x, y, z \in F$.*

(*a*) *If $x > 0$ and $y < z$, then $x \cdot y < x \cdot z$.*

(*b*) *If $x < 0$ and $y < z$, then $x \cdot z < x \cdot y$.*

Proof of a. Let $x, y, z \in F$ be such that $x > 0$ and $y < z$. It follows from the latter condition by Definition 7.21a that $y + (-y) < z + (-y)$. Thus, by FA4 from Definition 7.8, we have $0 < z + (-y)$. This combined with the fact that $0 < x$ implies by Definition 7.21b that $0 < x \cdot (z + (-y))$. Consequently, from Definition 7.8, we have

$$\begin{aligned} 0 &< x \cdot z + x \cdot (-y) && \text{FA9} \\ 0 &< x \cdot z + (-(x \cdot y)) && \text{Lemma 7.19} \\ 0 + x \cdot y &< (x \cdot z + (-(x \cdot y))) + x \cdot y && \text{Definition 7.21a} \\ 0 + x \cdot y &< x \cdot z + (-(x \cdot y) + x \cdot y) && \text{FA2} \\ 0 + x \cdot y &< x \cdot z + 0 && \text{FA4} \\ x \cdot y &< x \cdot z && \text{FA3} \end{aligned}$$

□

Proof of b. Let $x, y, z \in F$ be such that $x < 0$ and $y < z$. It follows from the former condition by Lemma 7.23 that $0 < -x$. Thus, by Lemma 7.24a, $(-x) \cdot y < (-x) \cdot z$. Consequently, from Definition 7.8, we have

$$\begin{aligned} -(x \cdot y) &< -(x \cdot z) && \text{Lemma 7.19} \\ -(x \cdot y) + (x \cdot y + x \cdot z) &< -(x \cdot z) + (x \cdot y + x \cdot z) && \text{Definition 7.21a} \\ -(x \cdot y) + (x \cdot y + x \cdot z) &< -(x \cdot z) + (x \cdot z + x \cdot y) && \text{FA1} \\ (-(x \cdot y) + x \cdot y) + x \cdot z &< (-(x \cdot z) + x \cdot z) + x \cdot y && \text{FA2} \\ 0 + x \cdot z &< 0 + x \cdot y && \text{FA4} \\ x \cdot z &< x \cdot y && \text{FA3} \end{aligned}$$

□

Remark 7.25. An immediate consequence of this lemma is the fact that if x and y are both positive or both negative, their product is positive.

Lemma 7.26. *Let F be an ordered field, and let $x \in F$. Then $0 \leq x^2$. Moreover, if $x \neq 0$, then $0 < x^2$.*

Proof. We divide into two cases ($x = 0$ and $x \neq 0$). Suppose first that $x = 0$. Then by Theorem 7.13, $0 \leq 0 = 0 \cdot 0 = 0^2 = x^2$, as desired. Now suppose that $x \neq 0$. We divide into two cases again ($x > 0$ and $x < 0$). If $x > 0$, then by Lemma 7.24a, $x > 0$ and $0 < x$ imply that $x \cdot 0 < x \cdot x$, from which it follows by Theorem 7.13 that $0 < x^2$, as desired. On the other hand, if $x < 0$, then by Lemma 7.24b, $x < 0$ and $x < 0$ imply that $x \cdot 0 < x \cdot x$, from which it follows for the same reason as before that $0 < x^2$, as desired. Both cases together prove the first statement, while the second case alone proves the second statement. □

Corollary 7.27. *Let F be an ordered field. Then $0 < 1$.*

Proof. By FA10 from Definition 7.8, $1 \neq 0$. Thus, by Lemma 7.26, $0 < 1^2 = 1$, as desired. □

Theorem 7.28. *If F is an ordered field, then F has no first or last point.*

Proof. Suppose for the sake of contradiction that F has a first point a. By Corollary 7.27, we have that $0 < 1$, which implies by Lemma 7.23 that $-1 < 0$. It follows by Definition 7.21a that $-1 + a < 0 + a$. Thus, by FA3 from Definition 7.8, $-1 + a < a$. Since there exists an object in F (namely $-1 + a$) that is less than a, Definition 3.3 tells us that a is not the first point of F, a contradiction.

The proof is symmetric in the other case. □

Theorem 7.29. *The rational numbers $\mathbb{Q}$ form an ordered field.*

Proof. To prove that $\mathbb{Q}$ forms an ordered field, Definition 7.21 tells us that it will suffice to show that $\mathbb{Q}$ forms a field; has an ordering $<$; satisfies $x+z<y+z$ if $x<y$ for all $z\in\mathbb{Q}$; and satisfies $0<x\cdot y$ if $0<x$ and $0<y$. We will take this one constraint at a time.

To show that $\mathbb{Q}$ forms a field, Definition 7.8 tells us that it will suffice to verify that $\mathbb{Q}$ has two binary operations ($+$ and $\cdot$), and satisfies field axioms 1-10. Define $+$ and $\cdot$ as in Definition 2.7. Under these definitions, parts a-i of Theorem 2.10 guarantee that $\mathbb{Q}$ satisfies FA1-FA9, respectively. As to FA10, to verify that $\left[\frac{1}{1}\right]\neq\left[\frac{0}{1}\right]$, Exercise 2.6 tells us that it will suffice to confirm that $(1,1)\nsim(1,0)$. But since $1\cdot 0=0\neq 1=1\cdot 1$, Exercise 2.2e confirms that $(1,1)\nsim(1,0)$, as desired.

$\mathbb{Q}$ has an ordering by Exercise 3.9d, as desired.

To show that $x+z<y+z$ if $x<y$ for all $z\in\mathbb{Q}$, let $\left[\frac{a}{b}\right],\left[\frac{c}{d}\right],\left[\frac{x}{z}\right]$ be arbitrary elements of $\mathbb{Q}$ with positive denominators (we can choose these WLOG by Exercise 3.9b) and the first two satisfying $\left[\frac{a}{b}\right]<\left[\frac{c}{d}\right]$; we seek to verify that $\left[\frac{a}{b}\right]+\left[\frac{x}{z}\right]<\left[\frac{c}{d}\right]+\left[\frac{x}{z}\right]$. Since $\left[\frac{a}{b}\right]<\left[\frac{c}{d}\right]$, we have by Exercise 3.9c that $ad<bc$. It follows by Script 0 that

$$\begin{aligned} ad &< bc \\ adzz &< bczz \\ adzz+bdxz &< bczz+bdxz \\ azdz+bxdz &< bzcz+bzdx \\ (az+bx)(dz) &< (bz)(cz+dx) \end{aligned}$$

Thus, by Exercise 3.9c, $\left[\frac{az+bx}{bz}\right]<\left[\frac{cz+dx}{dz}\right]$. Therefore, by Definition 2.7, $\left[\frac{a}{b}\right]+\left[\frac{x}{z}\right]<\left[\frac{c}{d}\right]+\left[\frac{x}{z}\right]$, as desired.

To show that $0<x\cdot y$ if $0<x$ and $0<y$, let $\left[\frac{a}{b}\right],\left[\frac{c}{d}\right]$ be arbitrary elements of $\mathbb{Q}$ with positive denominators (which we can choose for the same reason as before) such that $\left[\frac{0}{1}\right]<\left[\frac{a}{b}\right]$ and $\left[\frac{0}{1}\right]<\left[\frac{c}{d}\right]$; we seek to verify that $\left[\frac{0}{1}\right]<\left[\frac{a}{b}\right]\cdot\left[\frac{c}{d}\right]$. Since $\left[\frac{0}{1}\right]<\left[\frac{a}{b}\right]$ and $\left[\frac{0}{1}\right]<\left[\frac{c}{d}\right]$, we have by Exercise 3.9c that $0\cdot b<1\cdot a$ and $0\cdot d<1\cdot c$. It follows by Script 0 that $0\cdot bd<1\cdot ac$. Thus, by Exercise 3.9c, $\left[\frac{0}{1}\right]<\left[\frac{ac}{bd}\right]$. Therefore, by Definition 2.7, $\left[\frac{0}{1}\right]<\left[\frac{a}{b}\right]\cdot\left[\frac{c}{d}\right]$, as desired. ☐

2/4: **Definition 7.31.** We define $\oplus$ on $\mathbb{R}$ as follows. Let $A,B\in\mathbb{R}$ be Dedekind cuts. Define

$$A\oplus B=\{a+b\mid a\in A\text{ and }b\in B\}$$

Exercise 7.32.

(a) Prove that $A\oplus B$ is a Dedekind cut.

(b) Prove that $\oplus$ is commutative and associative.

(c) Prove that if $A\in\mathbb{R}$, then $A=\mathbf{0}\oplus A$.

Proof of a. To prove that $A\oplus B$ is a Dedekind cut, Definition 6.1 tells us that it will suffice to show that $A\oplus B\neq\emptyset$; $A\oplus B\neq\mathbb{Q}$; if $r\in A\oplus B$ and $s\in\mathbb{Q}$ satisfy $s<r$, then $s\in A\oplus B$; and if $r\in A\oplus B$, then there is some $s\in A\oplus B$ with $s>r$. We will take this one claim at a time.

To show that $A\oplus B\neq\emptyset$, Definition 1.8 tells us that it will suffice to find an element of $A\oplus B$. Since A,B are Dedekind cuts, Definition 6.1 asserts that they are nonempty. Thus, there exist rational numbers $x\in A$ and $y\in B$. Therefore, by the definition of $A\oplus B$, the sum $x+y\in A\oplus B$, as desired.

To show that $A\oplus B\neq\mathbb{Q}$, Definition 1.2 tells us that it will suffice to find an element of $\mathbb{Q}$ that is not an element of $A\oplus B$. For an analogous reason to before, we can choose $x,y\in\mathbb{Q}$ such that $x\notin A$ and $y\notin B$. It follows by Lemma 6.2 and Definition 5.6 that $x\geq a$ for all $a\in A$ and $y\geq b$ for all $b\in B$. Thus, by Script 0, $x+y\geq a+b$ for all $a+b\in A\oplus B$. Consequently, $x+y+1>x+y\geq a+b$ for all $a+b\in A\oplus B$, implying by Definition 3.1 that $x+y+1\neq a+b$ for any $a+b\in A\oplus B$. Therefore, $x+y\notin A\oplus B$, as desired.

To show that if $r\in A\oplus B$ and $s\in\mathbb{Q}$ satisfy $s<r$, then $s\in A\oplus B$, we let $r\in A\oplus B$ and $s\in\mathbb{Q}$ be arbitrary elements of their respective sets that satisfy $s<r$ and seek to verify that $s\in A\oplus B$. Since $r\in A\oplus B$, $r=x+y$ for some $x\in A$ and $y\in B$. Additionally, it follows from the fact that $s<r$ that

$s = r - q = x + y - q$ for some $q \in \mathbb{Q}^+$. Since $y \in B$ and $y - q \in \mathbb{Q}$ satisfy $y - q < y$, we have by Definition 6.1b that $y - q \in B$. Therefore, $s = (x) + (y - q)$ is an element of $A \oplus B$, as desired.

To show that if $r \in A \oplus B$, then there is some $s \in A \oplus B$ with $s > r$, we let $r \in A \oplus B$ and seek to find such an s. Since $r \in A \oplus B$, $r = x + y$ for some $x \in A$ and $y \in B$. It follows from the fact that $x \in A$ by Definition 6.1c that there exists a $z \in A$ with $z > x$. Consequently, by Script 0, $z + y > x + y$ is the desired element of $A \oplus B$. □

Proof of b. To prove that $\oplus$ is commutative, Definition 7.1 tells us that it will suffice to show that for all $A, B \in \mathbb{R}$, we have $A \oplus B = B \oplus A$. Let A, B be arbitrary elements of $\mathbb{R}$. Then by Definition 7.31, we clearly have

$$\begin{aligned} A \oplus B &= \{a + b \mid a \in A \text{ and } b \in B\} \\ &= \{b + a \mid b \in B \text{ and } a \in A\} \\ &= B \oplus A \end{aligned}$$

To prove that $\oplus$ is associative, Definition 7.1 tells us that it will suffice to show that for all $A, B, C \in \mathbb{R}$, we have $(A \oplus B) \oplus C = A \oplus (B \oplus C)$. Let A, B, C be arbitrary elements of $\mathbb{R}$. Then by Definition 7.31, we clearly have

$$\begin{aligned} (A \oplus B) \oplus C &= \{a + b \mid a \in A \text{ and } b \in B\} \oplus C \\ &= \{d + c \mid d \in \{a + b \mid a \in A \text{ and } b \in B\} \text{ and } c \in C\} \\ &= \{d + c \mid d = a + b \text{ for some } a \in A \text{ and } b \in B, \text{ and } c \in C\} \\ &= \{a + b + c \mid a \in A \text{ and } b \in B \text{ and } c \in C\} \\ &= \{a + e \mid a \in A, \text{ and } e = b + c \text{ for some } b \in B \text{ and } c \in C\} \\ &= \{a + e \mid c \in C \text{ and } e \in \{b + c \mid b \in B \text{ and } c \in C\}\} \\ &= A \oplus \{b + c \mid b \in B \text{ and } c \in C\} \\ &= A \oplus (B \oplus C) \end{aligned}$$

□

Proof of c. To prove that for all $A \in \mathbb{R}$, $A = \mathbf{0} \oplus A$, we will show for an arbitrary $A \in \mathbb{R}$ that every element of A is an element of $\mathbf{0} \oplus A$ and vice versa. Let A be an arbitrary element of $\mathbb{R}$. Suppose first that $x \in A$. Then by Definition 6.1c, there exists $y \in A$ such that $y > x$. Let $z = x - y$. Clearly, $z \in \mathbb{Q}$ and $z < 0$, so we know that $z \in \mathbf{0}$. Additionally, since $x - z = y$, we know that $x - z \in A$. Therefore, since $x = (z) + (x - z)$, we have by Definition 7.31 that $x \in \mathbf{0} \oplus A$. Now suppose that $z \in \mathbf{0} \oplus A$. Then by Definition 7.31, $z = x + y$ for some $x \in \mathbf{0}$ and $y \in A$. Since $x \in \mathbf{0}$, we know that $x < 0$, which means that $y > z$. This combined with the fact that $y \in A$ and $z \in \mathbb{Q}$ implies by Definition 6.1b that $z \in A$. □

7.2 Discussion

1/28:
- Script 6 journals due Wednesday.
- We'll also have to prove a density lemma:
  - Let X be a dense subset of a continuum C. Show that for all $x, y \in X$, if $x < y$, then there exists a $z \in X$ such that $x < z < y$.
  - Mark in Exercise 6.16 as "Density Lemma."
- Explicitly cite Field Axioms as you go.

2/2:
- For Theorem **??** in class, he wants a simple explanation of what the injective map looks like and why, but not a full-on rigorous proof.
  - Nothing in the journal for Theorem **??**, though.

- He also wants to see Theorems **??** and **??** in the journal.
- For Corollary 7.15, we can write that $x^{-1} \cdot x = 1$ and $x^{-1} \cdot (x^{-1})^{-1} = 1$, and know by the uniqueness of multiplicative inverses (Theorem 7.14) that $x = (x^{-1})^{-1}$. For Corollary 7.11, we have an analogous proof.
- Alternate Theorem 7.17:

$$\begin{aligned} 1 &= 1 \cdot 1 \\ &= (a \cdot a^{-1})(b \cdot b^{-1}) \\ &= (ab)(a^{-1}b^{-1}) \\ &= 0 \end{aligned}$$

- Alternate Lemma 7.18: $a + (-a) = 0$. $a + (-1)a = a(1 + (-1)) = a \cdot 0 = 0$. Thus, by Theorem 7.10, $-a = (-1)a$.
- Alternate Lemma 7.19: We can use the uniqueness of additive inverses (Theorem 7.10).
- We can also cite Remark 7.25 in Lemma 7.26.