

An Independent Axiom System for the Real Numbers

Greg Oman



Greg Oman (goman@otterbein.edu) is a visiting instructor at Otterbein College in Westerville, Ohio. He obtained his Ph.D. in 2006 from The Ohio State University, and currently works in several areas of mathematics including ring theory, semigroup theory, and logic. When not doing math, he enjoys working out, traveling, and playing with The Sweet.

The reals, of course, already have an axiom system. They are a complete, linearly ordered field. This axiom system is even *categorical*, meaning that it completely characterizes the reals. Up to isomorphism, the reals are the *only* complete, linearly ordered field.

Another property of axiom systems, considered to be particularly elegant ever since the birth of formal logic, is independence. In an *independent* axiom system no axiom is redundant; that is, no axiom may be proved from the remaining axioms. An early example of an independent axiom system is the set of axioms developed by David Hilbert for Euclidean geometry. In chapter two of [7], Hilbert carefully proved each of his axioms independent of the others by finding a model for the other axioms in which each chosen axiom was false. Since then, independent axioms systems have been found for such algebraic entities as fields [2] and vector spaces [9]. Hilbert's axioms for Euclidean geometry, incidentally, are categorical as well as independent.

The purpose of this paper is to describe an independent, categorical axiom system for the reals.

A categorical axiom system has a maximum property. No new axiom can be consistently added to such a system that is not already a consequence of the other axioms. An independent axiom system has a minimum property. No axiom can be subtracted from such a system and still be a consequence of the remaining axioms. Thus, an independent, categorical axiom system is a rather special mathematical object, a kind-of max-min or min-max system.

Hilbert's axiom system for Euclidean geometry is not often used. Its special qualities make it unsuitable for teaching. Other systems—one developed by CUPM, for example—have supplanted it, although it still appears in some geometry classes.

Likewise, it is unlikely that the axiom system presented here will supplant the concept of a complete, linearly ordered field. The latter system has many convenient features and is comparatively easy to teach. Still, it seems only fair that the real numbers, the foundation of so much mathematics, including all of analysis, should be accorded the same privilege as the (equally fundamental) theory of Euclidean geometry, and thus be given an independent, categorical axiomatization.

The axioms

We begin by stating the standard axioms for the real numbers as given in most real analysis texts.

Definition 1. A *complete ordered field* is a 6-tuple $(F, +, \cdot, 0, 1, <)$ where F is a set, $+$ and \cdot operations on F , 0 and 1 elements of F , and $<$ a binary relation on F satisfying the following axioms:

- (1) $1 \neq 0$,
- (2) (Associative Law for Addition) $a + (b + c) = (a + b) + c$ for all $a, b, c \in F$,
- (3) (Commutative Law for Addition) $a + b = b + a$ for all $a, b \in F$,
- (4) (Additive Identity) $a + 0 = a$ for all $a \in F$,
- (5) (Additive Inverses) For each $a \in F$ there is an element $b \in F$ such that $a + b = 0$,
- (6) (Associative Law for Multiplication) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in F$,
- (7) (Commutative Law for Multiplication) $a \cdot b = b \cdot a$ for all $a, b \in F$,
- (8) (Multiplicative Identity) $a \cdot 1 = a$ for all $a \in F$,
- (9) (Multiplicative Inverses) For each $a \in F - \{0\}$ there is an element $b \in F$ such that $a \cdot b = 1$,
- (10) (Distributive Law) $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$,
- (11) $<$ is a transitive relation on F ,
- (12) $<$ satisfies trichotomy on F ,
- (13) $x < y$ implies $x + z < y + z$ for every $x, y, z \in F$,
- (14) $x < y, z > 0$ imply that $x \cdot z < y \cdot z$ for every $x, y, z \in F$,
- (15) (Completeness) Every nonempty subset A of F that has an upper bound in F has a least upper bound in F .

We now present an alternative list of axioms, equivalent to the usual axiomatization of \mathbb{R} , but minimal in the sense that none of the axioms may be proved from the remaining ones. Preliminarily we call a model of the following axioms a *complete ordered algebra*.

Definition 2. A *complete ordered algebra* is a 5-tuple $(A, +, \cdot, 0, <)$ consisting of a set A , operations $+$ and \cdot on A , an element $0 \in A$, and a relation $<$ on A which satisfies the following axioms:

- (S1) A contains an element x besides 0 ,
- (A1) $+$ is associative,
- (A2) $a + 0 = a$ for all $a \in A$,
- (A3) For all $a \in A$ there exists $b \in A$ with $a + b = 0$,
- (D) For all $a, b, c \in A$: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$,
- (O1) $<$ is a transitive relation on A ,
- (O2) $<$ satisfies trichotomy on A ,
- (O3) If $a < b$, then $a + c < b + c$ and $c + a < c + b$ for all $a, b, c \in A$,
- (O4) If $a < b$ and $c > 0$, then $a \cdot c < b \cdot c$ and $c \cdot a < c \cdot b$ for all $a, b, c, \in A$,
- (O5) For all $x > 0$ there is a y such that $0 < y < x$,
- (C) Every nonempty subset of A that has an upper bound in A has a least upper bound in A .

Compared with the axioms for a complete ordered field, the axioms for a complete ordered algebra favor order over algebra. For example, the new system does not assume

commutativity of addition. Nor does it assume commutativity, or even associativity of multiplication, or the existence of a multiplicative identity, or multiplicative inverses. Remarkably, these multiplicative field axioms can, in the context of a complete ordered algebra, all be deduced as theorems. To balance the omission of so much algebra, two forms of ‘completeness’ are assumed, order completeness (C) and the Archimedean property (O5).

The axioms are categorical

We will prove that the complete ordered field of real numbers is the unique model of a complete ordered algebra up to isomorphism. We begin with two lemmas which will be useful later. The first is a well-known group-theoretic result. We include the easy proof.

Lemma 1. *Suppose $(S, +, 0)$ is a structure satisfying (A1), (A2), and (A3). Then S is a group.*

Proof. Let $x \in S$ be arbitrary. By (A3), there is a $y \in S$ with $x + y = 0$. Add y on the left to obtain $y + x + y = y + 0$. By (A2), we see that $y + 0 = y$. Thus $y + x + y = y$. By (A3), there exists some $z \in S$ with $y + z = 0$. Adding z on the right to both sides of the equation $y + x + y = y$, we obtain $y + x + y + z = y + z$. Using the fact that $y + z = 0$, the equation reduces to $y + x + 0 = 0$. By (A2), this reduces to $y + x = 0$. We have shown that every element of S has a two-sided inverse with respect to 0 . It remains to show that 0 is a two-sided identity. Let $x \in S$. We must show that $0 + x = x$. Let $y \in S$ be such that $x + y = y + x = 0$. Now simply note that $0 + x = (x + y) + x = x + (y + x) = x + 0 = x$. This completes the proof. ■

Our next lemma is a special case of a slightly more general result known as Hion’s Theorem. We sketch the main ideas of the proof, and refer the reader to [1, p. 147] for further details.

Lemma 2. *Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be an additive homomorphism. Suppose further that whenever $x < y$, then $f(x) < f(y)$ (f is increasing). Then there exists some real number $c \in \mathbb{R}$ such that $f(x) = cx$ for all $x \in \mathbb{R}$.*

Sketch of Proof. Trivially $f(1) = f(1) \cdot 1$ and $f(0) = f(1) \cdot 0$. It follows by induction that $f(n) = f(1) \cdot n$ for all positive integers n . If $n \in \mathbb{Z}$ and $n < 0$, then $f(n) = -f(-n) = -f(1)(-n) = f(1) \cdot n$. It is straightforward to extend this result to \mathbb{Q} ; that is, $f(q) = f(1) \cdot q$ for all $q \in \mathbb{Q}$. Since f is increasing and $0 < 1$, $f(0) = 0 < f(1)$. It follows that $\{f(1) \cdot q : q \in \mathbb{Q}\}$ is dense in \mathbb{R} . Using this fact along with the fact that f is increasing, it follows that $f(x) = f(1) \cdot x$ for all $x \in \mathbb{R}$. ■

The following corollary is a simple consequence of the previous lemma.

Corollary 1. *Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be an additive homomorphism. Suppose that whenever $x < y$, then $f(x) > f(y)$ (f is decreasing). Then there exists some real number $c \in \mathbb{R}$ such that $f(x) = cx$ for all $x \in \mathbb{R}$.*

We now prove two propositions which are the meat of our classification result. The proof of the first proposition follows closely the proof of Theorem 25.4 of [1, p. 149].

Proposition 1. Let \circ be an operation on \mathbb{R} which satisfies (D) (with respect to the usual addition on \mathbb{R}) and (O4) (with respect to the standard order on \mathbb{R}). Then the structures $(\mathbb{R}, +, \cdot, <)$ and $(\mathbb{R}, +, \circ, <)$ are isomorphic.

Proof. To be clear, we will denote the standard multiplication on \mathbb{R} by juxtaposition. Let $a \in \mathbb{R}$ be arbitrary. Note that $a \circ 0 = a \circ (0 + 0) = (a \circ 0) + (a \circ 0)$. Hence $a \circ 0 = 0$. Now define a function $f_a : \mathbb{R} \rightarrow \mathbb{R}$ by $f_a(x) := a \circ x$. We claim that there is some real number r_a such that $f_a(x) = r_a x$. If $a = 0$, then from what was shown above, we can take $r_a = 0$. Suppose now that $a > 0$. Since \circ satisfies (D) and (O4), it is easy to see that f_a is an increasing homomorphism on \mathbb{R} . The existence of r_a now follows from Lemma 2. In case $a < 0$, the existence of r_a follows from Corollary 1. Note that $f_a(1) = r_a 1 = r_a$, and thus each r_a is uniquely determined. We now define $f : \mathbb{R} \rightarrow \mathbb{R}$ by $f(a) := r_a$. We claim that f is an increasing additive homomorphism on \mathbb{R} . We first show that f is increasing. For suppose that $a < b$. We must show that $r_a < r_b$. Since \circ satisfies (O4), we have $a \circ 1 < b \circ 1$. But then by definition, $f_a(1) < f_b(1)$, and we get $r_a < r_b$. We now claim that $f_{a+b} = f_a + f_b$ for all real numbers a and b . To see this, simply note that $f_{a+b}(x) = (a + b) \circ x = a \circ x + b \circ x = f_a(x) + f_b(x)$. We can now show that f is a homomorphism as follows:

$$f(a + b) = r_{a+b} = f_{a+b}(1) = f_a(1) + f_b(1) = r_a + r_b = f(a) + f(b).$$

It follows again from Lemma 2 that there is some real number $c > 0$ such that $f(a) = ca$ for all $a \in \mathbb{R}$. It is now immediate that f is a bijection from \mathbb{R} onto \mathbb{R} . We have seen above that f is an order-preserving additive homomorphism. Thus to show that the structures $(\mathbb{R}, +, \cdot, <)$ and $(\mathbb{R}, +, \circ, <)$ are isomorphic, it suffices to show that $f(a \circ b) = f(a)f(b)$ for all $a, b \in \mathbb{R}$. Note from above that $a \circ b = f_a(b) = r_a b = f(a)b = cab$. Thus we have: $f(a \circ b) = f(cab) = c(cab) = c^2 ab = (ca)(cb) = f(a)f(b)$, and hence f is an isomorphism. ■

Our second proposition is a special case of Hölder's Theorem. We outline a proof and refer the reader to [1, p. 144] for further details.

Proposition 2. Let G be a group, and suppose that $(G, +, <)$ satisfies (S1), (O1)–(O3), (O5), and (C). Then $(G, +, <)$ is isomorphic to $(\mathbb{R}, +, <)$.

Sketch of Proof. Fix an arbitrary $a > 0$ in G . For any $b \geq 0$ in G , let

$$b^* := \left\{ \frac{m}{n} \in \mathbb{Q} : ma \leq nb, m \geq 0, n > 0 \right\}.$$

Note that $0 \in b^*$ and so b^* is not empty. The completeness of $<$ (in G) implies that $b \leq ka$ for some positive integer k (the proof is analogous to showing that the natural numbers are not bounded above in \mathbb{R}). It follows from this fact that b^* is bounded above in \mathbb{R} , and so $\sup(b^*)$ exists. We now let $G^+ := \{g \in G : g \geq 0\}$, and define $f : G^+ \rightarrow \mathbb{R}$ by $f(b) = \sup(b^*)$. Now extend f to all of G by defining $f(-g) := -f(g)$ for $g > 0$. Then f is an isomorphism between $(G, +, <)$ and a substructure $(H, +, <)$ of the real numbers. Since $(G, +, <)$ satisfies (S1), H is nontrivial. Since (O5) is satisfied, H is not cyclic. It follows that H is dense in \mathbb{R} . Since H is complete with the induced order, $H = \mathbb{R}$. This completes the proof. Note that both completeness assumptions were used. ■

Finally, we are in position to prove that the reals are the unique model of the axioms for a complete ordered algebra.

Theorem 1. *Every complete ordered algebra is isomorphic to the complete ordered field of real numbers.*

Proof. Let $(A, +, \odot, 0, 1, <)$ be a complete ordered algebra. It follows from Lemma 1 that $(A, +, 0)$ is a group. It now follows from Proposition 2 that $(A, +, <)$ is isomorphic to $(\mathbb{R}, +, <)$. Let $f : A \rightarrow \mathbb{R}$ be an isomorphism. We define an operation \circ on \mathbb{R} via this isomorphism by $x \circ y := f(f^{-1}(x) \odot f^{-1}(y))$. It is straightforward to verify that $(A, +, \odot, <)$ is isomorphic to $(\mathbb{R}, +, \circ, <)$. It now follows from Proposition 1 that the structures $(\mathbb{R}, +, \cdot, <)$ and $(\mathbb{R}, +, \circ, <)$ are isomorphic. Thus, finally, we see that the structures $(A, +, \odot, <)$ and $(\mathbb{R}, +, \cdot, <)$ are isomorphic. This completes the proof. ■

The axioms are independent

In the previous section, we showed that one can “throw away” many of the standard axioms for the real numbers. We now show that we cannot throw away any more axioms from our system. The standard method for doing this is, for each axiom φ , to create a model in which all the axioms of a complete ordered algebra hold except φ . Within the following models, 0 will denote the real number zero, 1 will denote the real number one, + and \cdot will denote the usual operations of addition and multiplication on \mathbb{R} , and $<$ will denote the usual ordering on \mathbb{R} (unless otherwise stated).

Proposition 3. *(S1) is independent.*

Proof. Let $(F, +, \cdot, 0, <) := (\{0\}, +, \cdot, 0, \emptyset)$. That every axiom holds but (S1) is easy to check. ■

Proposition 4. *(A1) is independent.*

Proof. Let $(F, +, \cdot, 0, <) := (\mathbb{R}, \oplus, \cdot, 0, <)$ where \oplus is defined by $a \oplus b = 2(a + b)$ if a and b are either both positive or both negative, and $a \oplus b = a + b$ otherwise. Clearly (S1), (O1), (O2), (O4), (O5), and (C) hold in this structure.

Note that (A1) fails here as follows: $1 \oplus (2 \oplus 3) = 1 \oplus 10 = 22$, but $(1 \oplus 2) \oplus 3 = 6 \oplus 3 = 18$, so \oplus is not associative.

(A2) holds. To see this, note that for any real number x , it is not the case that both x and 0 are positive, nor is it the case that both x and 0 are negative. Hence $x \oplus 0 = x + 0 = x$.

(A3) holds. Consider any real number x . Then as above, it is not the case that both x and $-x$ are positive nor is it the case that both x and $-x$ are negative. Hence $x \oplus -x = x + -x = 0$.

(D) holds. First note that as \cdot is commutative, we only need to check the first of the two equations. Hence consider arbitrary $a, b, c \in \mathbb{R}$. We will show $a(b \oplus c) = ab \oplus ac$.

Suppose first that $a = 0$. Simply note that $0b \oplus 0c = 0 \oplus 0 = 0 = 0(b \oplus c)$. Thus we now assume that $a \neq 0$ and consider two cases:

Case 1. b and c are either both positive or both negative. Then note that $a(b \oplus c) = a(2(b + c)) = 2ab + 2ac = 2(ab + ac) = ab \oplus ac$ (recall that since $a \neq 0$, ab and ac are also either both positive or both negative).

Case 2. b and c are not both positive and not both negative. Then note that $a(b \oplus c) = a(b + c) = ab + ac = ab \oplus ac$ (note again that if b and c are not both positive and not both negative, then the same is true of ab and ac since $a \neq 0$).

(O3) holds. Suppose that $a < b$ and consider an arbitrary element $c \in \mathbb{R}$. Since \oplus is commutative, we must only check that $a \oplus c < b \oplus c$. If $a \oplus c = a + c$ and $b \oplus c = b + c$ or if $a \oplus c = 2(a + c)$ and $b \oplus c = 2(b + c)$, we are clearly done. Hence we have two cases to consider:

Case 1. $a \oplus c = 2(a + c)$ and $b \oplus c = b + c$. Thus a and c are either both positive or both negative, but this is not true of b and c . Now, a and c cannot both be positive. If so, then as $a < b$, then b and c would both be positive, contradicting our assumption that $b \oplus c = b + c$. Hence a and c are both negative now follows from our assumption about b and c . It follows that $b \geq 0$. But since a and c are both negative, it follows that $2a + c < 0 \leq b$. Hence $2a + c < b$. Adding c to both sides yields $2(a + c) < b + c$, which is $a \oplus c < b \oplus c$, as required.

Case 2. $a \oplus c = a + c$ and $b \oplus c = 2(b + c)$. The proof in this case proceeds exactly as in Case 1 and is omitted. This completes the proof of the independence of (A1). ■

Proposition 5. (A2) is independent.

Proof. Let $(F, +, \cdot, 0, <) := (\mathbb{R}, +, \cdot, 1, <)$. One checks immediately that all axioms are satisfied except (A2). ■

Proposition 6. (A3) is independent.

Proof. Let $(F, +, \cdot, 0, <) := (\{x \in \mathbb{R} : x \geq 0\}, +, \cdot, 0, <)$. One checks immediately that all axioms are satisfied except (A3). ■

Proposition 7. (D) is independent.

Proof. Let $(F, +, \cdot, 0, <) := (\mathbb{R}, +, +, 0, <)$. It follows easily that all axioms are satisfied except for (D). ■

Proposition 8. (O1) is independent.

Proof. Let \mathbb{F}_7 denote the field with seven elements and define P by $P := \{\bar{1}, \bar{2}, \bar{4}\}$. Note that P enjoys the following properties:

- (i) P is closed under multiplication
- (ii) $P, \{0\}, -P$ forms a partition of \mathbb{F}_7

Now define a relation $<$ on \mathbb{F}_7 as follows:

$$x < y \Leftrightarrow y - x \in P \tag{1}$$

and let $(F, +, \cdot, 0, <) := (\mathbb{F}_7, +, \cdot, 0, <)$ (where, of course, $+$ and \cdot are the field addition and multiplication on \mathbb{F}_7). We will show that this structure satisfies all the axioms but transitivity of $<$.

It is clear that (S1), (A1)–(A3), and (D) hold.

(O1) does not hold. Using the definition (1), we see that $\bar{1} < \bar{2}$ and $\bar{2} < \bar{4}$, but $\bar{1} \not< \bar{4}$, so $<$ is not transitive.

(O2) holds. Consider any two elements x and y in \mathbb{F}_7 . Then since $P, \{0\}, -P$ forms a partition of \mathbb{F}_7 , we see that exactly one of $y < x, y = x, x < y$ holds. Thus (O2) holds in this structure.

(O3) holds. Suppose that $a < b$. We must show that $a + c < b + c$ for an arbitrary $c \in \mathbb{F}_7$. (We only need verify this inequality since $+$ is commutative) Simply observe that by definition, $a + c < b + c$ iff $(b + c) - (a + c) \in P$ iff $b - a \in P$ iff $a < b$.

(O4) holds. Suppose that $a < b$ and that $c > 0$. We must show that $ac < bc$ (and only this inequality since \cdot is commutative). We have by definition of $<$ that $b - a \in P$ and $c \in P$. Since P is closed under multiplication, $(b - a)c \in P$. But then this shows that $bc - ac \in P$. By definition, this means $ac < bc$.

(O5) holds. Simply note that the only positive elements are, by definition, $\bar{1}, \bar{2}$, and $\bar{4}$. Also note that from the definition, $\bar{4} < \bar{1}, \bar{1} < \bar{2}$, and $\bar{2} < \bar{4}$.

(C) holds. To see this, we first make a definition. For $a \in \mathbb{F}_7$, we let $U_a := \{x \in \mathbb{F}_7 : x \leq a\}$. Hence U_a is the set of elements that a bounds above. A straightforward calculation reveals the following:

$$U_{\bar{0}} = \{\bar{0}, \bar{3}, \bar{5}, \bar{6}\},$$

$$U_{\bar{1}} = \{\bar{0}, \bar{1}, \bar{4}, \bar{6}\},$$

$$U_{\bar{2}} = \{\bar{0}, \bar{1}, \bar{2}, \bar{5}\},$$

$$U_{\bar{3}} = \{\bar{1}, \bar{2}, \bar{3}, \bar{6}\},$$

$$U_{\bar{4}} = \{\bar{0}, \bar{2}, \bar{3}, \bar{4}\},$$

$$U_{\bar{5}} = \{\bar{1}, \bar{3}, \bar{4}, \bar{5}\},$$

$$U_{\bar{6}} = \{\bar{2}, \bar{4}, \bar{5}, \bar{6}\}.$$

Suppose now that $S \subseteq \mathbb{F}_7$ is any nonempty set bounded above. We must show that S has a least upper bound. (Note that this does not follow immediately from the finiteness of S . There are examples of finite non-transitively ordered sets which are bounded above with no least upper bound.) Since S is bounded above, it follows that $S \subseteq U_x$ for some $x \in \mathbb{F}_7$. Thus S has at most 4 elements. Suppose S is a singleton $\{y\}$. Then by trichotomy y is trivially a least upper bound for S . Suppose that S has exactly two elements a and b . Then we may assume $a < b$. But then b is a least upper bound for S by trichotomy again. If S has 3 or 4 elements, then it is easy to see from the previous list that x is the *only* upper bound of S , hence trivially must be the least upper bound. This proves that (C) holds and completes the proof of the proposition. ■

Proposition 9. (O2) is independent.

Proof. Simply let $(F, +, \cdot, 0, <) := (\mathbb{R}, +, \cdot, 0, \emptyset)$. ■

Proposition 10. (O3) is independent.

Proof. Let $(F, +, \cdot, 0, <) := (\mathbb{R}, +, \cdot, 0, P)$ where P is defined as follows: For real numbers x and y , define xPy iff either:

- (i) $x \leq 0$ and $x < y$ or
- (ii) $x > 0, y > 0$, and $y < x$

We have several axioms to check.

(O1) holds. To see this, suppose that xPy and yPz . We must show that xPz . Conditions (i) and (ii) above yield 4 cases to consider.

Case 1. $x \leq 0, x < y, y \leq 0, y < z$: then $x \leq 0$ and $x < z$. Thus by definition, we have xPz .

Case 2. $x \leq 0, x < y, y > 0, z > 0, z < y$: we have $x \leq 0$ and $z > 0$. Thus $x < z$. But then $x \leq 0$ and $x < z$, and so by definition we have xPz .

Case 3. $x > 0, y > 0, y < x, y \leq 0, y < z$: this is contradictory and not an actual possibility.

Case 4. $x > 0, y > 0, y < x, y > 0, z > 0, z < y$: then observe that $x > 0, z > 0$, and $z < x$. Hence by definition we again obtain xPz .

(O2) holds. Consider two distinct real numbers x and y . Then we may assume that $x < y$. If $x \leq 0$, then we see by definition that xPy . Otherwise, $x > 0$. But then $x > 0, y > 0$, and $x < y$. Thus by definition we have yPx . Hence any two real numbers are equal or compare under P . It is clear that the relation P is irreflexive. Hence as P is transitive, it follows that P satisfies trichotomy on \mathbb{R} .

(O3) fails. Observe that by definition $0P1$, but $1P2$ does not hold.

(O4) holds. Suppose that aPb and $0Pc$. We must show $acPbc$. Note by definition that $0Pc$ is equivalent to $0 < c$. We now look at both possibilities for aPb . Suppose that $a \leq 0$ and $a < b$. Then $ac \leq 0$ and $ac < bc$. But then by definition, $acPbc$. Suppose instead that $a > 0, b > 0$, and $b < a$. Then $ac > 0, bc > 0$, and $bc < ac$. Hence again by definition we obtain $acPbc$. This proves that (O4) holds.

(O5) holds. Suppose $0Px$. We must find a y with $0Py$ and yPx . Since $0Px$, we see that $0 < x$. Simply pick any y with $x < y$. Then it follows that $0Py$ and yPx .

(C) holds. Let S be any nonempty subset of \mathbb{R} bounded above with respect to the ordering P . We distinguish two cases:

Case 1. $S \subseteq (-\infty, 0]$ (here $(-\infty, 0]$ is defined with respect to the usual order $<$ on \mathbb{R}). Then the ordering P on S coincides with the usual order $<$ on \mathbb{R} . Thus the least upper bound of S with respect to P is equal to the least upper bound of S with respect to $<$ and we are done.

Case 2. S contains strictly positive elements. Recall that positive with respect to P coincides with positive with respect to $<$. By hypothesis, S is bounded above with respect to P . Let u be an arbitrary upper bound. If s is any positive element of S , then sPu . But then by definition, $s > 0, u > 0$, and $u < s$. In particular, u is a lower bound (with respect to $<$) of the collection of positive elements of S . Let u^* be the greatest lower bound (with respect to $<$) of the collection of positive elements of S . Then it is easy to see that u^* is a least upper bound of S with respect to the order P . This completes the proof. ■

Proposition 11. (O4) is independent.

Proof. Define an ordering P on the reals by xPy iff $y < x$. Then note that under this ordering $0P(-1)$. If (O4) held, then we could multiply through by -1 to obtain $0P1$. But then by definition, this would mean that $1 < 0$, which is absurd. Thus (O4) does not hold. It is a triviality to check the remaining axioms. ■

Proposition 12. *(O5) is independent.*

Proof. Simply consider the structure $(F, +, \cdot, 0, <) := (\mathbb{Z}, +, \cdot, 0, <)$. ■

Proposition 13. *(C) is independent.*

Proof. Let $(F, +, \cdot, 0, <) := (\mathbb{Q}, +, \cdot, 0, <)$. ■

We have now proved the following theorem.

Theorem 2. *The axioms for a complete ordered algebra are independent.*

Acknowledgments. The author wishes to thank the referees and the editor for helpful suggestions which greatly improved the exposition of this article.

References

1. M. Darnel, *Theory of Lattice-Ordered Groups*, Marcel Dekker Press, New York, 1995.
2. R. M. Dicker, A set of independent axioms for a field and a condition for a group to be the multiplicative group of a field, *Proc. London Math. Soc.* (3) **18** (1968) 114–124.
3. J. A. Dyer, A note on redundancies in the axiom system for the real numbers, *Amer. Math. Monthly* **74** (1967) 1244–1246.
4. H. Enderton, *Elements of Set Theory*, Academic Press, New York, 1977.
5. L. Fuchs, *Partially Ordered Algebraic Systems*, Pergamon Press, Reading MA, 1963.
6. A. Gleason, *Fundamentals of Abstract Analysis*, Addison-Wesley, Reading MA, 1966.
7. D. Hilbert, *The Foundations of Geometry*, Open Court Publishing, London, 1902.
8. Y. Hion, Archimedean ordered rings, *Uspékhí Mat. Nauk (N.S.)* **9** (1954) 237–242.
9. R. Miron and F. Radó, On the definitions of a module and a vector space by independent axioms, *Mathematica (Cluj)* **18** (1976) 179–186.

Proof Without Words: Powers of Two



$$1 + 1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n$$

—James Tanton (djamestanton@stmarksschool.org)

[James Tanton teaches at St. Mark’s School in Southborough MA. He is founder of the St. Mark’s Institute of Mathematics, which is dedicated to sharing the joy of doing mathematics, and he is keen on bridging the disconnect between high school and college mathematics cultures.]