Section 1.3: The Completeness of the Real Numbers

October 19, 2011

Abstract

There is one final axiom to add to those already studied (the axioms of an ordered field being a group of reals under addition, a monoid under multiplication, multiplicative inverses (when able, i.e. $x \neq 0$), distributivity, and the order axiom establishing the positive numbers and the law of trichotomy).

There are "holes" in the set of rational numbers – interesting numbers that aren't rational. This completeness axiom merely asserts that all the holes are filled in for the real numbers (with the additional of the irrational numbers).

1 Completeness

The problem: if we start with the ring of integers, which the Pythagoreans loved (except for that $x = 0$ thing, which came later), and then add in the divisors (except when $x = 0$), and decide which integers are positive, we've got a wonderful ordered field (the rationals). The Pythagoreans are still happy: everything is integers, or ratios of integers. Then, one dark and stormy night, they discovered holes in their number (and hence their whole philosophical) system: they discovered that $\sqrt{2}$ is irrational – can't be represented as ratios of whole numbers.

Question: Do you know how to prove that? [The usual proof uses contradiction, and requires you to know that a rational can be represented as a quotient of integers in lowest terms (numerator and denominator have no common prime factors).]

Definition: upper bound, bound above: Let A be a set of real numbers. If there is a real number b for which $x \leq b$ for every $x \in A$, then b is said to be an upper bound for A. A set that has an upper bound is said to be **bounded above**.

Definitions for **lower bound** and **bounded below** are the obvious analogues.

To do: Write them down by analogy.

To do: Draw a picture to represent both cases.

Definition: least upper bound, supremum: Let A be a set of real numbers that is bounded below. The number b is called the **least upper bound** (or **supremum** of the set A (denoted $lub(A)$ or $sup(A)$) if

(I) b is an upper bound of A, and

(II) If c is also an upper bound of A, then $b \leq c$.

Definitions for **greatest lower bound** and **infimum** are the obvious analogues.

To do: Write them down by analogy.

Definition: complete: Let S be an ordered field. Then S is said to be **complete** if for any nonempty subset A of S that is bounded above, the least upper bound of A is in S.

Observe: The rational numbers do not form a *complete* ordered field (just an ordered field).

Axiom of Completeness: The real number are complete.

Theorem 1-14: If the least upper bound and greatest lower bound of a set of real numbers exist, they are unique.

Observe: In the previous section, we defined powers when the exponent was **rational**: we now extend that definition to include irrational powers.

Definition: x^r **:** Let $x > 1$ be a positive real number and r a positive irrational number. Then the number x^r is the least upper bound of the set A where

$$A = \{x^p | p \text{ is a positive rational number less than } r\}$$

Theorem 1-15:

(I) A number α is the least upper bound of a set of real numbers A if and only if

  (a) α is an upper bound of A, and

  (b) Given an $\varepsilon > 0$, there is a number $x(\varepsilon)$ in A for which $x(\varepsilon) > \alpha - \varepsilon$.

(II) Similarly for the greatest lower bound.

To do: Write the definition in this case.

Proof: Let's prove this. Since this is a bi-directional (iff) theorem, we need to prove it in both directions:

(I) $\rightarrow$:

We assume that α is the $lub(A)$. As a lub, it is an upper bound, so it's the second part that we must establish: that is, that given an $\varepsilon > 0$, there is a number $x(\varepsilon)$ in A for which $x(\varepsilon) > \alpha - \varepsilon$.

We do this by contradiction. Assume not. Then there is no number $x(\varepsilon)$ in A with $x(\varepsilon) > \alpha - \varepsilon$. But then $\alpha - \varepsilon$ is a smaller lower bound than α, which is a contradiction to the assertion that α is the $lub(A)$.

(II) $\leftarrow$:

Now, let's assume that α is an upper bound of A, and that given an $\varepsilon > 0$, there is a number $x(\varepsilon)$ in A for which $x(\varepsilon) > \alpha - \varepsilon$. We need to show that α is the $lub(A)$.

Again, let's do it by contradiction. Assume that α is not the $lub(A)$. Then there is an upper bound smaller than α (call it $\overline{\alpha}$). Now let $\varepsilon = \alpha - \overline{\alpha}$; by assumption, there is a number $x(\varepsilon)$ in A for which $x(\varepsilon) > \alpha - \varepsilon = \overline{\alpha}$. But this contradicts the assumption that $\overline{\alpha}$ is an upper bound.

Q.E.D.

Theorem 1-16: Let $\alpha = lub(A)$, and $\alpha \notin A$. Then $\forall\varepsilon > 0$, the interval $(\alpha - \varepsilon, \alpha)$ contains an infinite number of points of A.

Proof: : I want to do this by contradiction. Let $\alpha = lub(A)$, but that $\alpha \notin A$. Now assume that there is some $\varepsilon > 0$ such that the interval $(\alpha - \varepsilon, \alpha)$ contains only a finite number of points of A. Then call the largest point $x(\varepsilon)$. Then $x(\varepsilon)$ is actually the least upperbound, since $x(\varepsilon) < \alpha$, and no $x \in A$ is greater (since α is an upperbound, and there is no other element in the interval $(\alpha - \varepsilon, \alpha)$. This is a contradiction, and the theorem is proved.

The author claims to do a proof by contraposition. I prefer a proof by contradiction, but that's just because I'm contradictory by nature...;). What's the difference?
Proof by contraposition:

$$(P \rightarrow Q) \longleftrightarrow (Q' \rightarrow P')$$

Proof by contradiction:

$$(P \rightarrow Q) \longleftrightarrow (P \wedge Q' \rightarrow 0)$$

Here's the theorem:

$$\alpha \equiv lub(A) \wedge (\alpha \notin A) \rightarrow (\forall\varepsilon)\left[(\varepsilon > 0) \rightarrow (\alpha - \varepsilon, \alpha) \text{ contains an infinite subset of } A\right]$$

Here's an equivalent version of the theorem (that we might use for the contraposition):

$$\alpha \equiv lub(A) \rightarrow ((\alpha \notin A) \rightarrow (\forall\varepsilon)\left[(\varepsilon > 0) \rightarrow (\alpha - \varepsilon, \alpha) \text{ contains an infinite subset of } A\right])$$

The author's proof by contraposition might be the following (in the domain of all upper bounds):

$$((\alpha \notin A) \rightarrow (\forall \varepsilon)\,[(\varepsilon > 0) \rightarrow (\alpha - \varepsilon, \alpha) \text{ contains an infinite subset of } A])' \rightarrow (\alpha \equiv lub(A))'$$

If you work out the negation on the left hand side, it comes to

$$(\alpha \notin A) \wedge (\exists \varepsilon)\,[(\varepsilon > 0) \rightarrow (\alpha - \varepsilon, \alpha) \text{ contains no infinite subset of } A] \rightarrow (\alpha \equiv lub(A))'$$

Now, what does our author assume? He picks a value of ε, which will ultimately create an interval that contains only a finite subset of A. Then he assumes the hypotheses $\alpha \equiv lub(A) \wedge (\alpha \notin A)$ (in order to determine that the interval $(\alpha - \varepsilon, \alpha)$ contains a point of A, for example). Then he assumes the negation of the conclusion (i.e., that there is only a finite number of elements of A in the interval). He then arrives at the conclusion that α is not the $lub(A)$ (i.e. he contradicts one of his hypotheses). Looks like a proof by contradiction to me....

Theorem 1-17: Let A be a bounded set of real numbers, and suppose c is a real number. Then

(I) If $c > 0$

  (a) $lub(c \cdot A) = c \cdot lub(A)$
  (b) $glb(c \cdot A) = c \cdot glb(A)$

(II) If $c < 0$

  (a) $lub(c \cdot A) = c \cdot glb(A)$
  (b) $glb(c \cdot A) = c \cdot lub(A)$

Theorem 1-18 (The Archimedean Principle): If a and b are real numbers with $a > 0$, then there is a positive integer n such that $na > b$.

Corollary 1-18: Let a be a positive real number and b be any real number. Then there is a positive integer n such that

$$\frac{b}{n} < a$$

2 Cardinality

The cardinality of a set measures its size. "Counting" for infinite sets is done via 1-1 correspondence: it two sets can be put into correspondence, then they are, in some sense, relabellings of each other.

Definition: cardinality, equivalent: Two sets A and B are said to have the same **cardinality** if there is a 1-1 onto function from the set A to the set B. In this case we say that A is **equivalent** to B.

Definition: finite with cardinality n, countable, uncountable: A set S is said to be **finite with cardinality** n if S is equivalent to $\{1, 2, 3, \ldots, n\}$. The empty set is finite with cardinality 0. Sets that do not have finite cardinality are **infinite** sets. A set S is called **countable** if it has the same cardinality as some subset of the positive integers. Sets that are not countable are said to be **uncountable.**

Observation: The smallest infinite set is the natural numbers, and its size is indicated using the Hebrew alphabet ($\aleph_0$ – pronounced "aleph-null").

Theorem 1-19: The union of a countable collection of countable sets is countable.

An example of such a collection is the lattice of points of the plane with natural numbered coordinates. The y-coordinate gives the set number, and the x-coordinate gives the ordered element in the countable set. Our author chooses a very nice 1-1 mapping **into** the natural number, which exploits the prime factorization theorem: he maps

$$(m, n) \rightarrow 2^m 3^n$$

It's 1-1 because $2^m 3^n = 2^M 3^N \iff (m = M) \wedge (n = N)$. It's into (and not onto) because no coordinate pair maps to 5, for example.

Observe: The rationals are countable. (This is a corollary of the Motel ∞ problem of the infinity (naturally numbered) of school buses, each with an infinity (naturally numbered) of seats, each fully occupied. The positive double infinite lattice of grid points in the plane with natural numbered coordinates – representing the buses and their seats – can be mapped **onto** the rationals. If set A can be mapped **onto** set B, then $Card(A) \geq Card(B)$ – can you prove that?)

Theorem 1-20: The real numbers in $(0, 1)$ form an uncountable set.

Observe: It's the **irrationals** that are uncountable – that overwhelm the Motel ∞. You can prove it informally to yourself by thinking of each in their popular personas: rationals are repeating decimals (possibly terminating – i.e., 0 repeats forever), and irrationals are non-repeating. If you had to throw a "10-sided die" to generate a random decimal .32421793817277...., what's the chance that it would be repeating? Let's suppose that it repeated a string of digits 100 long 4000 times. What's the chance that you could keep it up on the next throw? That's right – about zero.... So it's far easier to throw a non-repeating decimal expansion (i.e. irrational).

Theorem 1-21 (Cantor's Theorem): For X any set, let $\wp(X)$ denote the set of subsets of X. Then the cardinal number of $\wp(X)$ is strictly larger than the cardinal number of X.

Observe: The proof of Cantor's Theorem is a generalization of the diagonalization argument.

Observe: This means that there are an infinity of successively larger infinities: the power set of the reals is bigger than the reals: $Card(\wp(\mathbb{R})) > Card(\mathbb{R})$; $Card(\wp(\wp(R))) > Card(\wp(R))$; etc.

Note: A couple of notions you can rely on about infinity:

- a subset never has **greater** cardinality than the set itself.
- if there exists an onto map from A to B, then the cardinality of A is **at least** that of B.
- if there exists a 1-1 map from A to B, then the cardinality of A is **no more than** that of B.

Example: Exercise 9, p. 34 Let y be a positive real number, and let n be a positive integer. Let $A = \{x | x^n < y\}$.

(I) Show that A is nonempty and bounded above.

$0 \in A$, since $0^n = 0 < y$. Hence A is non-empty. Cases:

(a) Suppose $0 < y \leq 1$. Then $x \leq 1$ (by #8, p. 24): if $x > 1$, then $x^n > 1$; but $x^n < y$ – contradiction. Hence 1 is an upper bound on the set A.

(b) Suppose $y > 1$. Then y is an upper bound. If $x^n < y$, then $x \leq y$: otherwise, if $x > y$, then $x^n > y$ by induction. Base case: $x > y$. Consider $x^k > y$. Then $x^{k+1} > xy > y$. So $x^n > y$ for all $n \in \mathbb{N}$. But this is a contradiction.

(II) Let $z = lub(A)$. Show that $z^n = y$. Thus $z = y^{\frac{1}{n}}$, and we have proven Theorem 1-8.

Suppose that $z^n \neq y$. Then define $\varepsilon \equiv y - z^n > 0$. We proceed by induction, using the binomial theorem to find an element $z + \delta$ that slips between z^n and y, showing that $z \neq lub(A)$.

$$(z+\delta)^n = \sum_{k=0}^{n} \binom{n}{k} z^{n-k}\delta^k = z^n + \sum_{k=1}^{n} \binom{n}{k} z^{n-k}\delta^k = z^n + \delta \sum_{k=1}^{n} \binom{n}{k} z^{n-k}\delta^{k-1}$$

Now everything in the sum multiplied by δ in the final term can be bounded above. For example, we can always demand that $\delta < 1$, and we have an upper bound (call it α) on z. So we can assert that

$(z+\delta)^n \leq z^n + \delta \sum_{k=1}^{n} \binom{n}{k} \alpha^{n-k} \equiv z^n + \delta\beta$ where β is just some number, and δ must be chosen to be less than 1.

Now choose δ so that $\delta\beta < \varepsilon$ (and $\delta < 1$). We can always choose $\delta < min(\frac{\varepsilon}{\beta}, 1)$.

$$z^n < (z+\delta)^n \leq z^n + \delta \sum_{k=1}^{n} \binom{n}{k} \alpha^{n-k} = z^n + \delta\beta < z^n + \varepsilon < y$$

Hence, by definition, $z + \delta \in A$, which contradicts that $z = lub(A)$.

Now suppose that $z^n > y$. Then $z \notin A$, because it doesn't satisfy the definition of elements of A. Furthermore, there is no element of A within an ε-neighborhood of z, which is a contradiction of $z = lub(A)$.

Take $\varepsilon \equiv z^n - y$. Then using a similar application of the binomial theorem, we can show that, $\forall x \in A$, $\exists \delta > 0$ such that

$$(x + \delta)^n < x^n + \delta\beta < y + \varepsilon = z^n$$

But $(x+\delta)^n$ is not less than y, so $(x+\delta) \notin A$. Hence there is a gap between $x \in A$ and z, with no elements in it, so this contradicts $z = lub(A)$ (since, if $z \notin A$, $\exists$ an infinite number of elements in every $\varepsilon-$neighborhood of z).

Hence, by elimination, and the trichotomy property, $z^n = y$. **We have found an n^{th} root of y.**

(III) Let $B = \{x | x^n > y \wedge x > 0\}$. Show that B is nonempty and bounded below.

By definition elements of B satisfy $x > 0$. Hence B is bounded below by 0.

Now to show that B is nonempty. We need to find an element of B. Two cases: if $0 < y \leq 1$, we have that $1 \in B$ (since $1^n = 1 \geq y$). Suppose $y > 1$: then $y \in B$, since $y^n > y$ (by induction: $y > 1$; Suppose $y^k > y$; then $y^{k+1} > y^2 > y \cdot 1 = y$).

(IV) Now we want to show that $lub(A) = glb(B)$. Let $z \equiv glb(B)$. To show this we can simply show that z satisfies $z^n = y$. The proof is essentially the same as that for A above. We prove this by contradiction: assume not. Then either $z^n < y$ or $z^n > y$. Begin by assuming that $z^n < y$, and let $\varepsilon = y - z^n$. Then we can pass by the same process we did earlier to show that $\exists \delta > 0$ such that

$$z^n < (z + \delta)^n \leq z^n + \delta \sum_{k=1}^{n} \binom{n}{k} \alpha^{n-k} = z^n + \delta\beta < z^n + \varepsilon < y$$

Again, this shows that z is not the $glb(B)$, since $z + \delta$ is not an element of B – nor is any element in the interval $(z, z+\delta)$: since $z \notin B$ (since it doesn't meet the definition) and $z = lub(A)$, that neighborhood must contain an infinite number of points of B (by Theorem 1-16). This is a contradiction.

If $z^n > y$, then let $\varepsilon = z^n - y$, and consider $y^{\frac{1}{n}} + \delta$ (where by $y^{\frac{1}{n}}$ we mean the lub(A)). Using the binomial theorem in "the usual way", we have that

$$(y^{\frac{1}{n}} + \delta)^n \leq y + \delta\beta$$

and we can choose δ such that $\delta < \dfrac{\varepsilon}{\beta}$, so that

$$(y^{\frac{1}{n}} + \delta)^n < y + \varepsilon = z^n$$

Hence we have a contradiction of $z = glb(A)$, since $y^{\frac{1}{n}} + \delta \in B$, and $y^{\frac{1}{n}} + \delta < z$.

Thus, by the trichotomy, we have $z^n = y$, or $lub(A) = glb(B)$. Q.E.D.

In the end, we see that we are able to define n^{th} roots for any real number y (not just the rationals, as we did previously).