Section 1.2: The Real Numbers: An Ordered Field

October 19, 2011

Abstract

This section lays out the properties of the real numbers, which we will be exploring in the material to follow. In particular, we start with the notion that the reals are a particular type of algebraic structure, called a field. Fields have divisors. Furthermore, as you know, the real numbers have an ordering defined on them, and this ordering will be made more precise. The "distance function" (absolute value function) will be important to determine how far apart two reals are.

Induction is also introduced here, because we need it now.

1 Axioms of a Field

1. A field is a generalization of a ring;
2. a ring is a generalization of a group;
3. a group is a generalization of a monoid.

A group is a simple structure. Groups must satisfy four axioms:

1. Closure
2. Associativity
3. Identity element
4. Inverse elements

illustrated by an example of an important group: the group of permutations of a set.

Consider the set of students in this room. A permutation of the students rearranges them in their chairs, leading to a different configuration of the room. A permutation of a permutation is another permutation (compositions lead to members of the group). We can permute the students, then undo the permutation with another permutation (the inverse). There is also an identity permutation (no one moves!). That's all we need for a group.

In general, a group may be non-commutative: in this example, the order of permutations matters (the group is non-commutative). If I permute (swap) the positions of Jennifer and Chris, and then Chris and Amber, it's different from what happens if I swap the positions of Chris and Amber, then Jennifer and Chris.

A ring is a set R with two binary operations:

1. the binary operation of addition: $+ : R \to R$ (defined on the Cartesian product of R with itself); and

2. the binary operation of multiplication: $\cdot : R \to R$

$(R, +)$ is required to be an **abelian group** (that is, commutative group) under addition; and $(R, \cdot)$ is required to be a **monoid** under multiplication (that's a group, except that it doesn't necessarily have the inverses). Furthermore, the distributive law holds:

1. For all a, b and c in R, the equation $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ holds.

2. For all a, b and c in R, the equation $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ holds.

The integers under the usual operations of addition and multiplication is a commutative ring (meaning that $\cdot$ is also commutative – divisors are obviously a problem for integers!).

As we move from integers toward the reals, the multiplicative inverses exist, but if we start with the ring of integers, we'll only get the field of rational numbers by multiplicative inverses. It will be necessary to "complete" the reals.

Another problem for the real numbers, as we know, is that we can't divide by zero.... But we can still define inverses for all the other reals, so that completes the definition of the field (giving this distinguished additive identity 0 special place): for each $a \in F$ for which $a \neq 0$, there is a multiplicative inverse – that is, if $a \in F$ and $a \neq 0$, there is an element in F, denoted a^{-1} or $\frac{1}{a}$, for which $a \cdot a^{-1} = 1$.

Here are the axioms for the ordered field of the real numbers, spelled out:

- A1: $+$ and $\cdot$ are closed binary operations on the reals.
- A2: $+$ and $\cdot$ are associative.
- A3: $+$ and $\cdot$ are commutative.
- A4: Distributivity holds: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.
- A5: $\exists$ identities: $0 + a = a$ and $1 \cdot a = a$.
- A6: $\exists$ additive inverses.
- A7: $\exists$ multiplicative inverses (for $a \neq 0$).
- A8: $\exists$ non-empty subset $P \in \mathbb{R}$ such that the following hold:

$$\begin{array}{rcl} a, b \in P & \rightarrow & a + b \in P \\ a, b \in P & \rightarrow & a \cdot b \in P \\ a \in \mathbb{R} & \rightarrow & (a \in P) \vee (-a \in P) \vee (a = 0) \end{array}$$

Given these axioms, there are several theorems that we could immediately investigate:

1. Let F be a field. Then the identities are unique.
2. Let F be a field. Then the inverses are unique.
3. Let F be a field. Then $a \cdot 0 = 0$ for every $a \in F$.
4. Let F be a field. Then
   (a) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
   (b) $-(-a) = a$
   (c) $(-a) \cdot (-b) = a \cdot b$

Could you prove all of those? If not, which would cause you trouble?

2 The Order Axiom

Let F be a field. Then F is an ordered field if it satisfies the additional axiom: there is a nonempty subset P of F (called the positive subset) for which

1. If $a, b \in P$, then $a + b \in P$ (closure under addition)
2. If $a, b \in P$, then $ab \in P$ (closure under multiplition)
3. For any $a \in P$, exactly one of the following holds: $a \in P$, $-a \in P$, or $a = 0$ (law of trichotomy).

Definition: Let F be an ordered field, and let P be the positive subset of F. Let $a, b \in F$. We say $a < b$ if $b - a \in P$. We say $a \leq b$ if $a < b$ or $a = b$. The statements $a < b$ and $b > a$ are equivalent.

Theorem 1-7: Let F be an ordered field. For $a, b, c \in F$ the following hold:

1. If $a < b$, then $a + c < b + c$.
2. If $a < b$ and $b < c$, then $a < c$. (transitivity)
3. If $a < b$ and $c > 0$, then $ac < bc$.
4. If $a < b$ and $c < 0$, then $bc < ac$.
5. If $a \neq 0$, then $a^2 > 0$.

This could be called Brahmagupta's theorem (India, 7th century AD): he apparently used zero for the first time in a modern way, and wrote down these laws.

Theorem 1-8: Let $x \in \mathbb{R}_+^*$, $n \in \mathbb{N}$. Then there is a unique $y \in \mathbb{R}_+^*$ such that $y^n = x$. We define $y \equiv x^{1/n}$.

Theorem 1-9: Let $x \in \mathbb{R}_+^*$, and $s_1, s_2 \in \mathbb{N}$ such that $s_1 < s_2$. Then

1. $x > 1 \rightarrow x^{s_1} < x^{s_1}$
2. $0 < x < 1 \rightarrow x^{s_1} > x^{s_1}$

Theorem 1-10: Let $x, y \in \mathbb{R}_+^*$, with $x < y$, and let $s \in \mathbb{Q}_+^*$. Then $x^s < y^s$.

3 Mathematical Induction

Induction is a very beautiful and somewhat subtle method of proof: the idea is that we want to demonstrate a property associated with natural numbers (or a subset of the natural numbers). As a typical example, consider a theorem of the following type (which we might call "Gauss's theorem," hypothesized when he was seven or so):

Prove that the sum of the first n natural numbers is $\frac{n(n+1)}{2}$.

An induction proof goes something like this:

- We'll show that it's true for the first case (usually $k = 1$, called the base case). While the first case is often $k = 1$, this isn't mandatory: we simply need to be sure that there is a first case for which the property is true. $k = 0$ is another popular choice....
- Then we'll show that, if the property is true for the k^{th} case, then it's true for the $(k+1)^{th}$ case (the inductive step).
- Then we'll put them together: if it's true for 1, then it's true for 2; if it's true for 2, then it's true for 3; .... "to infinity, and beyond!" Or up the ladder, as our author would say.

Imagine dominoes falling. That's what it's like.

The most commonly used form of the principle of induction is expressed as follows:

First Principle of Mathematical Induction:

$$\left.\begin{array}{l} 1.\ P(1) \text{ is true} \\ 2.\ (\forall k)[P(k) \text{ true } \rightarrow P(k+1) \text{ true }] \end{array}\right\} \rightarrow P(n) \text{ true for all positive integers } n$$

Vocabulary:

- **inductive hypothesis**: $P(k)$
- **basis step** (base case, anchor): establish $P(1)$
- **inductive step** (implication): $P(k) \rightarrow P(k+1)$

Our author proves "Gauss's theorem" by induction: for any natural number n, $1+2+3+\ldots+n = \frac{n(n+1)}{2}$. He also proves properties of the binomial coefficients, and then the binomial theorem.

Let's do a different proof: let's prove that $2^{n-1} \leq n!$ for $n \geq 1$.

A Couple of Fun Examples:

1. The prisoner's last request (finite backwards induction!)

2. Let's use induction to prove an amazing fact: all horses are the same color.

   Proof: By induction, on the number of horses.

   Base case: 1 horse. No problem! Same color.

   Inductive step: we'll show that if it is true for any group of N horses, that all have the same color, then it is true for any group of $N+1$ horses.

   Well, given any set of $N+1$ horses, if you exclude the last horse, you get a set of N horses. By the inductive step these N horses all have the same color. But by excluding the first horse in the pack of $N+1$ horses, you can conclude that the last N horses also have the same color. Therefore all $N+1$ horses have the same color.

   QED – or have we?

4 The Absolute Value Function

This provides us with our *metric* (or measuring stick) for measuring distances along the real axis. It's funny, but this is one of the most misunderstood functions in calculus, primarily because of its definition:

Definition: The **absolute value** of $a \in \mathbb{R}$ is given by

$$|a| = \begin{cases} a & if\ a \geq 0 \\ -a & if\ a < 0 \end{cases}$$

Having that negative sign in there just seems to scream out at some folks that the absolute value can be negative. But that would be bad!

Theorem 1-13: The following hold for $a, b \in \mathbb{R}$:

1. $|a| \geq 0$, with equality iff $a = 0$.
2. $|a| = |-a|$.
3. $-|a| \leq a \leq |a|$.
4. $|ab| = |a| \cdot |b|$.

5. $1/|b| = |1/b|$ if $b \neq 0$.

6. $|a/b| = |a|/|b|$ if $b \neq 0$.

7. $|a| < b$ iff $-b < a < b$.

8. $|a + b| \leq |a| + |b|$ (the triangle inequality - draw the triangle!)

9. $||a| - |b|| \leq |a - b|$. (the signs can work for you, on the right)

A **metric** (or measuring stick) is defined by the three properties:

1. $d(a, b) \geq 0$, and $d(a, b) = 0 \iff a = b$.

2. $d(a, b) = d(b, a)$

3. $d(a, c) \leq d(a, b) + d(b, c)$.

The absolute value function can be used on the reals via the definition $d(a, b) = |a - b|$ to satisfy the definition of a metric.

Example: Exercise 15, p. 24 Prove by induction the following generalization of the triangle inequality:

$$|a_1 + a_2 + \ldots + a_n| \leq |a_1| + |a_2| + \ldots + |a_n|$$

where $a_i \in \mathbb{R}$.

Proof: We prove this by induction. The base case is the triangle inequality,

$$|a_1 + a_2| \leq |a_1| + |a_2|$$

which was proven as part of Theorem 1-13.

For the induction step, we need to assume P_k and show that P_{k+1} follows. So assume P_k:

$$|a_1 + a_2 + \ldots + a_k| \leq |a_1| + |a_2| + \ldots + |a_k|$$

Now consider

$$|a_1+a_2+\ldots+a_k+a_{k+1}| = |(a_1+a_2+\ldots+a_k)+a_{k+1}| \leq |a_1+a_2+\ldots+a_k|+|a_{k+1}|$$

by the base case. Then

$$|a_1 + a_2 + \ldots + a_k + a_{k+1}| \leq |a_1| + |a_2| + \ldots + |a_k| + |a_{k+1}|$$

by the induction hypothesis, and so we have demonstrated P_{k+1}. Hence, the result follows by induction.

Example: Exercise 18, p. 24 : Prove the Schwarz inequality: that

$$\sum_{i=1}^{n} a_i b_i \leq \left(\sum_{i=1}^{n} a_i^2\right)^{\frac{1}{2}} \left(\sum_{i=1}^{n} b_i^2\right)^{\frac{1}{2}}$$

We're given a hint: to consider $\sum_{i=1}^{n}(\alpha a_i - \beta b_i)^2 \geq 0$, and choose α and β wisely.

$$\sum_{i=1}^{n}(\alpha a_i - \beta b_i)^2 = \sum_{i=1}^{n}[\alpha^2 a_i^2 - 2\alpha\beta a_i b_i + \beta^2 b_i^2] = \alpha^2 \sum_{i=1}^{n} a_i^2 - \sum_{i=1}^{n} 2\alpha\beta a_i b_i + \beta^2 \sum_{i=1}^{n} b_i^2 \geq 0.$$

Hence

$$\alpha^2 \sum_{i=1}^{n} a_i^2 + \beta^2 \sum_{i=1}^{n} b_i^2 \geq 2\alpha\beta \sum_{i=1}^{n} a_i b_i$$

We need the right hand stuff – what will we do with the left? Choose

$$\alpha^2 = \frac{1}{\sum_{i=1}^{n} a_i^2} \qquad\qquad \beta^2 = \frac{1}{\sum_{i=1}^{n} b_i^2}$$

Then

$$1 + 1 \geq 2 \frac{1}{(\sum_{i=1}^{n} a_i^2)^{\frac{1}{2}}} \frac{1}{(\sum_{i=1}^{n} b_i^2)^{\frac{1}{2}}} \sum_{i=1}^{n} a_i b_i$$

or

$$\sum_{i=1}^{n} a_i b_i \leq \left(\sum_{i=1}^{n} a_i^2\right)^{\frac{1}{2}} \left(\sum_{i=1}^{n} b_i^2\right)^{\frac{1}{2}}$$

As for the question of when equality holds, we can go back to the hinted inequality, setting it to zero, and we'll see that we'll have equality when

$$a_i = \frac{\beta}{\alpha} b_i$$

(with $\frac{\beta}{\alpha} \geq 0$). If you'll recall your linear algebra, the quantity on the left is the inner product of vectors $\mathbf{a}$ and $\mathbf{b}$, whereas the right-hand side is the product of the norms of each vector....