13 Basic proofs involving real numbers [14]

In this chapter we begin the systematic study of the *real number system*. You've worked with for most of your life, consisting of the real numbers, the operations addition, multiplication, subtraction and division for combining numbers, and the relationship "less than" for comparing numbers. In past courses you've learned to apply universal principles about the real numbers. In this chapter, you'll begin to prove some of these universal principles.

13.1 The axiomatic approach

As usual, when we set out to develop a mathematical subject, we have to decide on a starting point. What facts and general principles about the real numbers can we assume, and which do we have to prove? Mathematicians like to find the smallest list of initial assumptions, and build up from there. This set of initial assumptions are called *axioms*. Here we'll present a standard set of axioms about the real numbers.

As you read through the axioms of the real numbers, you should think about the axioms from two different points of view:

The knowledgeable point of view Using all of your past knowledge about numbers,, you can see that each axiom (with the possible exception of the completeness axiom) is obviously true.

The "visitor from Mars" view Imagine that you are a visitor from Mars who knows the basics of logic, sets and functions covered in earlier chapters of this book, but never heard of the real numbers. The axioms of the real numbers give you the basic information, and that's all you know to start with. You can only use the axioms, or theorems you prove using the axioms.

To emphasize the "visitor from Mars" view, when we state the axioms we'll use the symbol S to represent the set rather than $\mathbb{R}$. So the system we consider will consist of a set S, together with two binary operations. called addition, and multiplication. We will use the normal symbols $+$ and $\times$ (or $\cdot$) to represent addition and multiplication, but in the "visitor from Mars" view you need to forget everything you know about addition and multiplication that is not part of the axioms.

The axioms are divided into three groups

Algebraic axioms These are the basic principles that govern equations.

Order axioms These are the basic principles that govern the "less than" relationship.

Completeness axiom There is one additional axiom that captures our intuition that when represented by a number line, the real numbers have "no gaps". This is the most technical axiom and will require careful discussion.

We proceed to discuss each set of axioms.

[14] Version 4/3/15.

13.2 The algebraic axioms

The algebraic properties are themselves divided into four groups: *closure properties of addition and multiplication*, *equality axioms of arithmetic*, *axioms of 0 and 1*, and *inverse axioms*

Closure properties of addition and multiplication

- *Closure under addition.* The sum of any two members of S is a member of S.
- *Closure under multiplication.* The product of any two members of S is a member of S.

These axioms restate the assumptions that $+$ and $\times$ are both binary operations on S.

Equality axioms of arithmetic These are the familiar properties that govern the way that arithmetic expressions can be reorganized.

- *Commutative Property of addition.* For all $x, y \in S$, $x + y = y + x$.
- *Associative Property of addition.* For all $x, y, z \in S$, $(x + y) + z = x + (y + z)$.
- Commutative Property of multiplication. For all real numbers x and y, $x \cdot y = y \cdot x$.
- Associative Property of multiplication. For all $x, y, z \in S$, $x \cdot (y \cdot z) = (x \cdot y) \cdot z$.
- Distributive Property of multiplication over addition. For all real numbers $x, y, z \in S$, $x \cdot (y + z) = x \cdot y + x \cdot z$ and $(y + z) \cdot x = y \cdot x + z \cdot x$.

Axioms of 0 and 1 Before stating these axioms, we need some definitions. We say that a member z of S is an *additive identity element* provided that for all $x \in S$, $x+z = z+x = x$. We say that a member y of S is a *multiplicative identity* provided that for all $x \in S$, $x \cdot y = y \cdot x = x$.

There are two special elements of S, denoted 0 and 1 with $0 \neq 1$ such that:

- *Axiom of 0.* 0 is an *additive identity element* of S.
- *Axiom of 1.* 1 is a *multiplicative identity element* of S.

Inverse axioms For $x \in S$, an *additive inverse* for x is a number that when added to x gives 0, and a *multiplicative inverse* for x is a number that when multiplied by x gives 1. We have two additional axioms:

- *Additive inverse axiom.* Every $x \in S$ has an additive inverse.
- *Multiplicative inverse axiom.* Every nonzero member x has a multiplicative inverse.

13.3 Building up from the algebraic axioms

The reader may notice that there lots of basic universal principles from algebra that are missing, such as: for all $x \in S$, $x \times 0 = 0$. Any such universal principle that is not an axiom must be provable from the axioms.

Also, some important concepts, such as subtraction and division, are missing. Since these operations are not part of the initial set of objects (the set S, the operations $+$ and $\times$) we must provide definitions for them in terms of the starting concepts and axioms.

In this subsection we'll show how this building up process is done. Here we take the "visitor from Mars" view, where we can only use the axioms or things we can prove from the axioms. We'll soon see that it is very tedious to state and prove all of the elementary universal principles that we'll want to be able to use later. So, after illustrating the building up process, we'll state some shortcuts that can be used later in writing proofs.

Additional properties of 0 Here are two important properties of 0 that are not part of the axioms.

Proposition 13.1. *1. For all $x \in S$, $x \cdot 0 = 0$ and $0 \cdot x = 0$.*

2. For all $x, y \in S$, if $x \cdot y = 0$ then $x = 0$ or $y = 0$.

Proof. Suppose x is an arbitrary member of S. Let w be an additive inverse of $x \cdot 0$. Then $x \cdot 0 = x \cdot 0 + 0 = x \cdot 0 + (x \cdot 0 + w)$. By associativity, this equals $(x \cdot 0 + x \cdot 0) + w$ and by the distributive law, this is equal to $x \cdot (0 + 0) + w$. Since 0 is an additive identity, this is equal to $x \cdot 0 + w$ which is 0 since w is an additive inverse of $x \cdot 0$. So $x \cdot 0 = 0$, and also by commutativity of multiplication, $0 \cdot x = 0$.

For the second part, suppose $x, y \in S$ and assume $x \cdot y = 0$. If $x = 0$ we 're done, so assume that $x \neq 0$. Then x has a multiplicative inverse we'll call z. Multiplying both sides of our equation by z we get $z \cdot (x \cdot y) = z \times 0$. The righthand side is 0 by the previous part of this proposition, so $z \cdot (x \cdot y) = 0$. Using associativity, the lefthand side equals $(z \cdot x) \cdot y = 1 \cdot y = y$. So $y = 0$, as required. □

Uniqueness of additive and multiplicative identity and additive and multiplicative inverses. Studying the axioms leads to some questions:

1. The axiom of 0 tells us that 0 is an additive identity element. Could there be more than one additive identity element?

2. The axiom of 1 tells us that 1 is a multiplicative identity element. Could there be more than one multiplicative identity element?

3. The additive inverse axiom says that every member x of S has an additive inverse. Can an element of S have more than one additive inverse?

4. The multiplicative identity element says that every non-zero member of S has a multiplicative inverse. Can an element of S have more than one multiplicative inverse?

The answers to these questions are given by the following:

Proposition 13.2. *(Uniqueness properties)*

1. *0 is the only additive inverse element.*

2. *1 is the only multiplicative inverse element.*

3. *Every element $x \in S$ has a unique additive inverse.*

4. *Every element $x \in S$ has a unique multiplicative inverse.*

Proof. We'll prove the first and third parts and leave the other two parts as exercises.

For the first part we know that 0 is an additive inverse and we want to show that there are no other additive inverses. Suppose z is an additive inverse. We must show $z = 0$. Consider $z + 0$. Since z is an additive inverse $z + 0 = 0$. Since 0 is an additive inverse, $z + 0 = z$. Therefore we have:

$$0 = z + 0 = z,$$

as required.

For the third part, suppose $x \in S$. By the additive inverse axiom, we know that x has an additive inverse. We need to show that there can be at most one additive inverse for x. Suppose that y and z are both additive inverses of x; we must show $y = z$. We'll do this by considering the sum $(y + x) + z$ and showing that this sum is equal to both y and z, and so $y = z$. We have $(y + x) + z = 0 + z = z$, using the fact that y is an additive inverse of x, and that 0 is an additive identity. Also $(y + x) + z = y + (x + z)$ by associativity. We then have $y + (x + z) = y + 0 = y$, since z is an additive inverse of x and 0 is an additive identity. Therefore $y = z$, as required. □

Exercise 13.1. Prove parts 2 and 4 of Proposition 13.2.

Since every element x of S has a unique additive inverse, we can talk about *the* additive inverse of x. Similarly if x is non-zero we can talk about *the* multiplicative inverse of x. It is useful to have a notation for the additive inverse and multiplicative inverse of x:

Definition 13.1. Suppose $x \in S$.

Definition of $-x$ We define $-x$ to mean the additive inverse of x.

Definition of $1/x$ For $x \neq 0$, we define $1/x$ to mean the multiplicative inverse of x.

Now there are a bunch of familiar rules that tell us how the additive and multiplicative inverse behave under various operations.

Proposition 13.3. *Suppose x and y are arbitrary real numbers.*

1. $-(x + y) = -x + -y$.

2. $-(x \cdot y) = -x \cdot y$ *and* $-(x \cdot y) = x \cdot -y$.

3. *If* x, y *and* $x \cdot y$ *are non-zero then* $1/(x \cdot y) = 1/x \cdot 1/y$.

4. *If* x, y *and* $x \cdot y$ *are non-zero then* $1/x + 1/y = (x + y) \times 1/(x \cdot y)$.

Proof. We'll prove the second statement, and leave the others as an exercise. Suppose x, y are arbitrary real numbers.By definition, $-(x \cdot y)$ is the additive inverse of $x \cdot y$. We'll show that $-x \cdot y$ and $x \cdot -y$ are also additive inverses of $x \cdot y$, and since the additive inverse of $x \cdot y$ is unique, they are both equal to $-(x \cdot y)$.

We have $x \cdot y + -x \cdot y = (x + -x) \cdot y$ by the distributive property, and this is $0 \cdot y = 0$. So $-x \cdot y$ is an additive inverse of $x \cdot y$. By a similar argument $x \cdot -y$ is also an additive inverse of $x \cdot y$. □

Exercise 13.2. Prove parts 1 and 3 of Proposition 13.2.

Definitions of subtraction and division For real numbers x and y:

- *Definition of subtraction* $x - y$ is defined to mean $x + (-y)$, which is the sum of x and the additive inverse of y.

- *Definition of division* $\frac{x}{y} = x/y = x \div y$ is defined to mean $x \cdot \frac{1}{y}$, which is the product of x and the multiplicative inverse of y.

Cancellation laws In high school algebra, students learn various ways that you can cancel operations from both sides of an equation:

Proposition 13.4. *For any real numbers* x, y, z*:*

1. *If* $x + z = y + z$ *then* $x = y$.

2. *If* $x - z = y - z$ *then* $x = y$.

3. *If* $x \cdot z = y \cdot z$ *and* $z \neq 0$ *then* $x = y$.

4. *If* $x/z = y/z$ *where* $z \neq 0$ *then* $x = y$.

Proof. We'll prove the first part and leave the rest as exercises. Suppose x, y, z are arbitrary real numbers. Assume $x + z = y + z$. Then $(x + z) + -z = (y + z) + -z$. Applying associativity to both sides we have $x + (z + -z) = y + (z + -z)$. By the definition of $-z$ we have $z + -z = 0$ and so $x + 0 = y + 0$. Since 0 is an additive identity, $x = y$. □

Exercise 13.3. Prove parts 2,3 and 4 of Proposition 13.4.

Using the equality axioms Students typically learn how to use the equality axioms in high school algebra. For example, consider the following familiar statement:

For all $x, y \in S$, $(x + y) \cdot (x + y) = x^2 + 2x \cdot y + y^2$.

This is not an axiom, so we have to prove it. Actually before we prove it, technically to *define* what we mean by x^2, since a visitor from Mars doesn't know what that means. In fact, we also have to define what "2" means, since 2 is not part of the axioms! So we define 2 to be 1+1. Also, for all $x \in S$ we define $x^2 = x \cdot x$.

More generally, we can define the natural numbers as follows

Now we can provide a proof of the above inequality from the axioms.

Proof. Suppose $x, y \in S$. Then $(x+y)\cdot(x+y) = (x+y)\cdot x+(x+y)\cdot y$, by the distributive axiom. Applying the distributive axiom again, this equals $x\cdot x+y\cdot x+x\cdot y+y\cdot y$. By the commutative property of multiplication, $y\cdot x = x\cdot y$, and so the sum is equal to $x\cdot x+x\cdot y+x\cdot y+y\cdot y$, and since 1 is a multiplicative identity, $x \cdot x + 1 \cdot (x \cdot y) + 1 \cdot (x \cdot y) + y \cdot y$, and by the distributive property this is equal to $x \cdot x + (1 + 1) \cdot (x \cdot y) + y \cdot y$. Using the definition of the number 2, and x^2 and y^2, this is equal to $x^2 + 2xy + y^2$. □

The previous examples show how we can start to build up all of the basic algebra facts you learned in high school from the axioms. We could continue this way, but it would be a long and tedious process. So we now provide a shortcut for writing proofs involving the algebraic properties.

Algebraic Manipulation Since elementary school, you've used the equality axioms of arithmetic to transform an arithmetic expression into an equal arithmetic expression. For example if a,b, c, d and m are real numbers, with $c \neq 0$, then a combination of these properties shows:

$$((ma - b) + md)/c = \frac{m}{c}(a + d) - \frac{b}{c}.$$

When you use the equality properties and definitions of subtraction and division in this way, it is usually not necessary to show each individual step. You can just justify the equation by saying that it is true by "algebraic manipulation".

13.4 Other algebraic systems

In describing the algebraic axioms of the real number, we used the letter S for the set of numbers rather than $\mathbb{R}$ to emphasize the "visitor from Mars" view. There's another reason. It turns out that there are other choices of the set S, and other ways to interpret + and × that give interesting mathematical systems that satisfy some or all of the axioms.

Example 13.1. If we let S be the set $\mathbb{Q}$ of rational numbers, then all of the algebraic axioms still hold.

Example 13.2. If we let S be the set $\mathbb{Z}$ of integers, then all of the algebraic axioms hold, except the existence of multiplicative inverses: It is not true that every non-zero integer has a multiplicative inverse that is an integer.

Example 13.3. Recall that if m is a positive integer, we defined the relation $\equiv_m$ on the set of integers by $j \equiv_m k$ if $(j-k)$ is divisible by m. We showed that this is an equivalence relation. Denote by $[j]$ the equivalence class of the integer j. We showed that each of the classes $[0], [1], \ldots, [m-1]$ is different, and every integer belongs to one of these classes. Thus the $\{[0], [1], \ldots, [m-1]\}$ is the set of all classes. In an exercise, you showed that we can define operations $+_m$ and $\times_m$ on this set so that for any i, j, we have $[i] + [j] = [i+j]$ and $[i] \times [j] = [i \times j]$.

For example when $m = 3$, the set of classes is $\{[0], [1], [2]\}$ and the operations are given by the following tables:

$+_3$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[0]	[2]	[0]
[2]	[2]	[0]	[1]

$\times_3$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

You can check that $\mathbb{Z}_3$ with these operations satisfies all of the algebraic axioms. Note that the [0] is the additive identity and [1] is the multiplicative identity. The additive inverse of [1] is [2] and both [1] and [2] are their own multiplicative inverse.

More generally, for any integer $m \geq 2$, $\mathbb{Z}_m$ satisfies all of the algebraic axioms except that there may be elements that dont have multiplicative inverses. The following proposition tells us when this happens.

Proposition 13.5. *For any integers m and j there is an integer i such that $ij \equiv_m 1$ if and only if j and m are relatively prime.*

Exercise 13.4. Prove Proposition 13.5.

Corollary 13.6. *For all integers $m \geq 2$, every non-zero member of $\mathbb{Z}_m$ has a multiplicative inverse if and only if m is prime.*

Exercise 13.5. Prove Corollary 13.5.

Example 13.4. Suppose n is a positive integer and let $\mathcal{M}_n$ denote the set of all $n \times n$ matrices with real entries. We define addition and multiplication operations for matrices by $A+B$ is the $n \times n$ matrix defined by the the rule $(A+B)_{i,j} = A_{i,j} + B_{i,j}$ for all $i, j \in \{1, \ldots, n\}$ and $A \times B$ is the matrix given by the rule $(A \times B)_{i,j} = \sum_{k=1}^{n} A_{i,k} B_{k,j}$. It can be shown that this system satisfies all of the algebraic axioms except that (1) Matrix multiplication is not commutative, and (2) Not all matrices have multiplicative inverses.

We have now seen various algebraic systems involving a set and two operations. We classify systems in the following way:

Field A system that satisfies all of the algebraic axioms is called a *field*. Thus $(\mathbb{R}, +, \times)$ is a field, $(\mathbb{Q}, +, \times)$ is a field and $(\mathbb{Z}_m, +_m, \times_m)$ is a field provided that m is prime. The algebraic axioms are also called the *field axioms*.

Ring A system that satisfies all of the algebraic axioms except (possibly) the axiom that multiplication is commutative, and the axiom that every non-zero element has a multiplicative inverse, is called a *ring*. All of the examples described above are rings.

Commutative Ring A ring where multiplication is commutative is called a *commutative ring*. A commutative ring satisifies all the algebraic axioms except (possibly) the axiom that all elements have multiplicative inverses.

So we see that many different systems that satisfy the algebraic (or field) axioms, all of which are fields. Any theorem we prove using only the field axioms will be satisfied by every field. We will need to add additional non-algebraic axioms to distinguish the real number system from other fields.

13.5 Summations and Products

When working with real numbers, we often want to add or multiply together a list of numbers or, more generally, an indexed collection with finite index set. There is a standard notation for this:

- $\sum_{i \in I} a_i$, which is read "the sum of a_i over all i in I" is the number obtained by adding together each of the a_i for i a member of I.
- $\prod_{i \in I} a_i$, which is read "the product of a_i over all i in I" is the number obtained by multiplying together each of the a_i for i a member of I.

The commutative and associative property of addition and multiplication can be used to show that the sum is independent of the order in which we add or multiply the elements of the list.

In the special case that I is a consecutive subset of integers, so that for some integers m and n, $I = \{i \in \mathbb{Z} : m \leq i \leq n\}$ we define the notation:

$$\begin{aligned} \sum_{i=m}^{n} a_i &= \sum_{i \in I} a_i \\ \prod_{i=m}^{n} a_i &= \prod_{i \in I} a_i. \end{aligned}$$

The summation $\sum_{i=m}^{n} a_i$ is sometimes written as:

$$a_m + a_{m+1} + \cdots + a_n.$$

We refer to this as dot-dot-dot notation for sums. One problem with dot-dot-dot notation is that it might not be clear what the pattern of terms is. If you write:

$$5 + 8 + \cdots + 32,$$

the reader may not know what you mean, while if you write $\sum_{j=1}^{10}(3j+2)$, the meaning is clear. So you should use dot-dot-dot notation only when you are confident that your meaning will be clear to the reader. The dot-dot-dot notation is sometimes easier to understand when working with simple sums (we'll see some examples below), but it is confusing for more complicated sums, such as when we have a double summation such as:

$$\sum_{i=1}^{n}\sum_{j=1}^{i} ij^2.$$

In dot-dot-dot notation this would be:

$$(1(1^2)) + (2(1^2) + 2(2^2)) + \cdots + (n(1^2) + n(2^2) + \cdots + n(n^2)).$$

which may be confusing or ambiguous to the reader.

The distributive law extends to products of sums as follows:

Proposition 13.7. *Suppose $(x_i : i \in I)$ and $(y_i : i \in J)$ are two finite indexed collections of real numbes. Then*

$$(\sum_{i\in I} x_i)(\sum_{j\in J} y_j) = \sum_{i\in I} x_i(\sum_{j\in J} y_j) = \sum_{j\in J} y_j(\sum_{i\in I} x_i) = \sum_{(i,j)\in I\times J} x_i y_j.$$

We frequenty use the notation $[n]$ to denote te set $\{1,\ldots,n\}$. Thus $\sum_{i=1}^{n} x_i = \sum_{i\in[n]} x_i$.

Corollary 13.8. *For any list $x_1,\ldots,x_n$ of numbers:*

$$(\sum_{i=1}^{n} x_i)^2 = \sum_{i=1}^{n} x_i^2 + 2\sum_{1\le i<j\le n} x_i x_j.$$

Modifying the index of summation In the sum $\sum_{i=1}^{n} x_i$, the index i is a dummy variable. We are free to change it to another letter: $\sum_{j=1}^{n} x_j$. Here we are making a substitution of j for i as the index of summation. We can also make a *shifted substition* such as $j = i + 3$. In that case the sum becomes $\sum_{j=4}^{n+3} x_{j-3}$. Notice that this sum is still equal to $x_1 + \cdots + x_n$.

This technique can be useful in combining and simplifying sums.

Example 13.5. Simplify $\sum_{i=1}^{n}(x_i - x_{i+1})$.
Solution $\sum_{i=1}^{n}(x_i - x_{i+1}) = \sum_{i=1}^{n} x_i - \sum_{i=1}^{n} x_{i+1}$. Shift the second summation by making the substitution $j = i+1$. Then the second sum becomes $\sum_{j=2}^{n+1} x_j$. Now replace j by i and combine with the first sum to get:

$$\sum_{i=1}^{n} x_i - \sum_{i=2}^{n+1} x_i.$$

Split the first sum into $x_1 + \sum_{i=2}^{n} x_i$ and split the second sum into $\sum_{i=2}^{n} x_i + x_{n+1}$. The two sums cancel each other leaving $x_1 - x_{n+1}$.

The previous example is a situation where dot-dot-dot notation may be easier to understand. If we write out the sum as:

$$(x_1 - x_2) + (x_2 - x_3) + \cdots + (x_n - x_{n+1}),$$

then we see that $-x_2$ is cancelled by x_2, $-x_3$ is cancelled by $-x_3$, etc. leaving only $x_1 - x_{n+1}$. This kind of sum is called a *telesoping sum* (because it collapses like a collapsible telescope).

The argument by telescoping may seem easier then the argument in the proof. Still it is important to learn the techniques used in the proof (changing index of summation, and breaking off terms of the summation), because these techniques are more reliable then telescoping when manipulating more complicated sums.

Proposition 13.9. *For any real numbers x and y and positive integer n we have:*

$$x^n - y^n = (x - y) \sum_{i=0}^{n-1} x^i y^{n-1-i}.$$

Proof. Suppose that x and y are arbitrary real numbers and n is an arbitrary positive integer. Consider the right hand side R of the desired equation:

$$\begin{aligned} R &= (x-y) \sum_{i=0}^{n-1} x^i y^{n-1-i} \\ &= \sum_{i=0}^{n-1} x^{i+1} y^{n-1-i} - x^i y^{n-i} \\ &= \sum_{i=0}^{n-1} x^{i+1} y^{n-1-i} - \sum_{i=0}^{n-1} x^i y^{n-i}. \end{aligned}$$

Change the index of summation in the first sum by making the substitution $j = i + 1$ and change the index of summation in the second sum by simply replacing j by i. As a result we get:

$$
\begin{aligned}
R &= \sum_{j=1}^{n-1} x^j y^{n-j} - \sum_{j=0}^{n-1} x^j y^{n-j} \\
&= x^n + \sum_{j=1}^{n-1} x^j y^{n-j} - \sum_{j=1}^{n-1} x^j y^{n-j} - y^n \\
&= x^n - y^n,
\end{aligned}
$$

as required to complete the proof. □

Exercise 13.6. Give an alternate proof using dot-dot-dot notation and telescoping sums.

13.6 Order properties of the real numbers

Besides algebraic properties of the reals, another important property is that the real numbers are totally ordered by the "less than or equal to" relationship. One important type of universal principles for numbers, consists of principles that say that under certain conditions one expression involving real numbers is less than, or less than or equal to, another expression involving the same variables. Here's a typical example of such a principle:

Theorem 13.10. *For any two vectors (lists) a and b of real numbers,*

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

In words this says that the square of the dot product of two vectors is at most the product of the square of their lengths. This theorem is important enough that it is called the *Cauchy-Schwartz inequality* after the mathematicians who discovered it. We'll prove this inequality (and others) below.

Before we begin proving inequalities, we need to lay the foundation by establishing the basic rules (axioms) about inequalities that we'll use. We start with the obvious: There is a total order $\leq$ on the set $\mathbb{R}$. This total order satisfies:

Preservation of inequality under addition For any $x, y, z \in \mathbb{R}$, if $x \leq y$ then $x+z \leq y+z$.

Product of nonnegatives For any $x, y \in \mathbb{R}$, if $x \geq 0$ and $y \geq 0$ then $xy \geq 0$.

We define the set $\mathbb{R}_+$ of *positive* numbers to be $\{x \in \mathbb{R} : x > 0\}$ and the set $\mathbb{R}_-$ of negative numbers to be $\{x \in \mathbb{R} : x < 0\}$.

As with the algebraic axioms, there are many basic facts that are not axioms, and can be proved using the axioms. Here is a partial list:

Proposition 13.11. *Let $x, y, z \in \mathbb{R}$.*

1. *If* $x \leq y$ *then* $x - z \leq y - z$.

2. *If* $x < y$ *then* $x + z < y + z$.

3. *If* $x \neq 0$ *then either* x *is positive and* $-x$ *is negative or* x *is negative and* $-x$ *is positive.*

4. *If* $x > 0$ *and* $y < 0$ *then* $xy < 0$.

5. *If* $x < 0$ *and* $y < 0$ *then* $xy > 0$.

6. *The square of any nonzero number is positive.*

7. 1 *is positive.*

Exercise 13.7. Prove Proposition 13.11

Proposition 13.12. *Suppose that* x, y, z, w *are arbitrary real numbers.*

1. *If* $x \leq y$ *and* $z \leq w$ *then* $x + z \leq y + w$.

2. *If* $x < y$ *and* $z \leq w$ *then* $x + z < y + w$.

3. *If* $x \leq y$ *and* $z \geq 0$ *then* $zx \leq zy$. *Equality holds if and only if* $x = y$ *or* $z = 0$.

4. *If* $x \leq y$ *and* $z > 0$ *then* $x/z \leq y/z$. *Equality holds if and only if* $x = y$.

5. *If* $x \leq y$ *and* $0 \leq w$ *then* $wx \geq wy$. *Equality holds if and only if* $x = y$ *and* $w = 0$.

6. *If* $x \leq y$ *and* $z \leq w$ *and* $x \geq 0$ *and* $w \geq 0$ *then* $zx \leq wy$.

Proof. Proof of 3. Assume $x \leq y$ and $z \geq 0$. then $y - x$ is positive or 0 and z is positive or 0. If $y - x$ is positive and z is positive, then so is $(y - x)z = yz - xz$ and so $yz > xz$. Otherwise $y - x = 0$ or $z = 0$ and so $(y - x)z = 0$ and so $yz = xz$.

The proofs of the remaining parts are left as an exercise. □

Exercise 13.8. Prove the remaining parts of Proposition 13.12.

Ordered fields. The set of real numbers satisfies the field axioms and the order axioms. There are other systems that satisfy the field and order axioms. We already observed that the set $\mathbb{Q}$ of rational numbers with the operations $+$ and $\times$ satisfies the field axioms, and it also satisfies the order axioms. A system that satisfies both the field and order axioms is called an *ordered field*. There are other ordered fields, but we won't discuss them here.

Since there are other ordered fields are not enough to specify the set of real numbers. To do this we'll need on more axiom, called the *completeness axiom*, which will be presented in Section 13.7.

Defining the integers We know that the integers are a subset of the real numbers. How can we describe the set of integers when we are working within the axioms?

If we have a system satisfying the ordered field axioms, the set of integers is a subset of this set. The set of nonnegative integers is obtained by starting with 0, and then including all number obtained by repeatedly adding 1. The set of integers is obtained by taking all nonnegative integers together with their additive inverses.

Here's a more formal definition:

Definition 13.2. Suppose $(S, +, \times)$ is an ordered field.

Inductive set We say that a subset T of S is *inductive* if it satisfies that for all $x \in T$ we have $x + 1 \in T$.

Nonnegative integers The set of nonnegative integers is the intersection of all inductive sets that contain 0.

Integers The set of integers consists of all nonnegative integers and negations of nonnegative integers.

13.7 The completeness axiom

The axioms that we've presented so far for the real numbers fall into two groups: the algebraic axioms, and order axioms. It turns out we'll need one more axiom. The form of this axiom is somewhat different from the others. Before stating the axiom, we'll discuss why we need another axiom.

Are these axioms enough? We'd like our set of axioms to be able to be sufficient to prove all true statements about the real number system. Here's a statement:

Assertion 13.1. (Square root principle for $\mathbb{R}$) For every $x \in \mathbb{R}$, if $x > 0$ there is a positive number $z \in \mathbb{R}$ such that $z^2 = x$. In other words, every positive real number has a positive square root.

This is certainly a property that we expect of the real number system. As we'll see: It is *impossible* to prove the square root principle from the algebraic axioms and the order axioms.

How can we know that it is impossible to prove the square root principle with just the algebraic and order axioms? It's one thing to say that we don't know how to prove the square root principle from the algebraic axioms and the order axioms. It's another thing to say that it's *not possible* to do this. How can we know such a thing? We know because there is a *mathematical proof* that it's impossible! The proof would require us t0 carefully discuss and develop ideas from the field of mathematical logic, which is outside the scope of this book. So rather than give a complete proof, we'll explain informally (without proof) the main idea of the proof.

We've already observed that the system consisting of the set $\mathbb{Q}$ with the operations $+$ and $\times$ satisfies the ordered field axioms.

Now suppose that we could prove the square root principle from the ordered field axioms. Since $\mathbb{Q}$ is an ordered field, we would then know that the square root principle also holds for $\mathbb{Q}$, that is, we'd have that every positive rational number has a rational number square root. But there's a problem: *The set $\mathbb{Q}$ does not satisfy the square root principle.* (We'll see why it doesn't in a moment.) Since the square root principle for $\mathbb{Q}$ is not true, it should not be possible to prove it. But we just said that if it's possible to prove the square root principle using only the ordered field axioms, then the square root principle must be true for $\mathbb{Q}$. We therefore have a contradiction, and conclude that such a proof is *not possible*.

Why is the square root principle for $\mathbb{Q}$ not true? To show that the square root principle for $\mathbb{Q}$ is not true, we have to show that there is a rational number that has no rational number square root.

For this proof we'll need the following simple fact: The product of two odd numbers is odd.

Exercise 13.9. Prove that the product of any two odd numbers is odd.

Theorem 13.13. *For any rational number r, $r^2 \neq 2$.*

Proof. Let r be a rational number. By definition of rational number, there are integers we'll call a and b such that $r = a/b$. By cancelling common factors in a and b we can assume that a and b have no common factor. Suppose for contradiction that $r^2 = 2$. Then $(a/b)^2 = 2$, so $a^2 = 2b^2$. So a^2 is even, and since the square of an odd number is odd, a must be even. So there is an integer we'll call k so that $a = 2k$. So $(2k)^2 = 2b^2$ and therefore $2k^2 = b^2$. But then we must also have b is even. But then a and b have a common factor of 2, contradicts our assumption that a and b have no common factor. Therefore $r^2 \neq 2$ and since r was an arbitrary rational number, we conclude that there is no rational number whose square is 2. $\square$

Since the square root principle can't be proved just using the ordered field axioms, we need at least one more axiom. This axiom is called the *completeness axiom.* We give three different versions of the completeness axiom. The first version is the most intuitive, but is not commonly used in other books. The second version is the version found in most books, and the third version is similar to the second version.

The Completeness Axiom.

Version 1:The betweenness axiom. Suppose that A and B are non-empty sets of real numbers such that for all $a \in A$ and $b \in B$ we have $a \leq b$. Then there is a number c that is *between* A and B, which means that for all $a \in A$ we have $a \leq c$ and for all $b \in B$ we have $c \leq b$.

Version 2:The least upper bound axiom. Suppose that S is a non-empty set of real numbers. If S has an upper bound, then it has a least upper bound.

Version 3: The greatest lower bound axiom. Suppose that S is a non-empty set of real numbers. If S has a lower bound, then it has a greatest lower bound.

Exercise 13.10. Prove that the three above axioms are equivalent. That is prove that if we assume that one of the axioms is true, then we can prove the other two.

Let's see how the completeness axiom is used to prove the square root principle. We'll prove a special case: That the number 2 has a square root, and leave the general case as an exercise.

Proof. Suppose x is an arbitrary positive real number. We'll prove that there is positive real number z such that $z^2 = 2$.

Let $A = \{y \in (0, \infty) : y^2 < 2\}$ and let $B = \{y \in (0, \infty) : y^2 > 2\}$.

We want to apply the betweenness axiom to A and B, so we need to check the hypotheses. It's easy to see that A and B are nonempty: $1 \in A$ and $2 \in B$. **Claim**: For all $a \in A$ and for all $b \in B$, $a \leq b$.

To prove the claim let $v \in A$ be arbitrary and $w \in B$ be arbitrary. Then $v^2 < 2 < w^2$, so $w^2 - v^2 > 0$. Therefore $(w - v)(w + v) > 0$, By definition of A and B, w and v are both positive so $w + v > 0$. Therefore $1/(w + v) > 0$. We can multiply both sides of the previous inequality by $1/(w + v)$ to get $w - v > 0$, and so $w > v$.

We have therefore shown that A and B satisfy the hypothesis of the betweenness axiom. So there is a number we'll call z so that for all $a \in A$ and $b \in B$, $a \leq z \leq b$. We claim $z^2 = 2$.

Suppose for contradiction that $z^2 \neq 2$. Then we have either $z^2 < 2$ or $z^2 > 2$. We'll show that $z^2 < 2$ is not possible, and leave as an exercise to show that $z^2 > 2$ is impossible.

Case 1. Assume $z^2 < 2$. We'll show that there is a member of A that is greater than z which would contradict that z is an upper bound on A. Note first that $z > 0$ (since $1 \in A$ and so $z \geq 1$). So it's enough to find a number $w > z$ so that $w^2 < 2$. This is equivalent to finding a number $\delta > 0$ so that $(z + \delta)^2 < 2$, and this condition is equivalent to $\delta^2 + 2z\delta < 2 - z^2$. We know $z < 2$ since $2 \in B$, so for any $\delta \in (0, 1)$ we know that $2\delta z + \delta^2 < 4\delta + \delta \leq 5\delta$. So if we choose $\delta = (2 - z^2)/5$ (which is a positive number) we'll have $2\delta z + \delta^2 < 2 - z^2$, as required. Thus we have that $(z + (2 - z^2)/5) \in A$ and is larger than z which gives a contradiction.

Case 2. Assume $z^2 > 2$.

Exercise 13.11. Show that case 2 leads to a contradiction.

Since cases 1 and 2 are impossible we conclude that $z^2 = 2$. □

Exercise 13.12.

By the same method one can prove the following more general fact (which should be familiar to most readers):

Theorem 13.14. *For any positive integer n:*

1. *If n is odd then for all real numbers x there is a unique real number y such that $y^n = x$.*

2. *If n is even then for all nonnegative real numbers x there is a unique nonnegative real number y such that $y^n = x$.*

Exercise 13.13. Prove Theorem 13.14

By Theorem 13.14, for each positive integer n we can define a function f_n such that if n is odd then $f_n : \mathbb{R} \longrightarrow \mathbb{R}$ and if n is even then $f_n : \mathbb{R}_{\geq 0} \longrightarrow \mathbb{R}_{\geq 0}$, and for all $x \in \mathbf{Dom}(f_n)$, $f_n(x)$ is the unique member of codomain of f_n such that $y^n = x$. We use the common notation $x^{1/n}$ to mean $f_n(x)$.

13.8 Increasing Functions

Suppose that $f : \mathbb{R} \longrightarrow \mathbb{R}$ is a function and $I = [a, b]$ is an interval. We say that:

- f *is increasing on* I if for all $x, y \in I$ with $x < y$ we have $f(x) < f(y)$.
- f *is decreasing on* I if for all $x, y \in I$ with $x < y$ we have $f(x) > f(y)$.
- f *is nondecreasing on* I if for all $x, y \in I$ with $x < y$ we have $f(x) \leq f(y)$.
- f *is nonincreasing on* I if for all $x, y \in I$ with $x < y$ we have $f(x) \leq f(y)$.

In calculus you may have learned to use the derivative to determine whether a function has one of these properties on a particular interval. Here we will investigate how to prove that a function is increasing without the aid of calculus.

Example 13.6. Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ denote the function given by $f(x) = x^2$. Prove that: (1) f is increasing on the interval $[0, \infty)$, and (2) f is decreasing on the interval $(-\infty, 0]$.

Proof. We'll prove (1) and leave (2) as an exercise. Suppose that $x, y \in [0, \infty)$ with $x < y$. We must show that $x^2 < y^2$ which is the same as showing $y^2 - x^2 > 0$. Since $y^2 - x^2 = (y - x)(y + x)$ and $y - x > 0$ and $y + x > 0$ (since $y > x \geq 0$) we have that $y^2 - x^2 > 0$ (since the product of positive numbers is positive. □

Theorem 13.15. *Let k be positive integer.*

1. *If k is even then the function given by $f(x) = x^k$ is an increasing function on the set $[0, \infty)$ and is a decreasing function on the set $(-\infty, 0]$.*
2. *If k is odd then the function given by $f(x) = x^k$ is increasing on all of $\mathbb{R}$.*

Exercise 13.14. Prove Theorem 13.15.

Proposition 13.16. *Let f be a function whose domain includes the interval $[a, b]$ such that $f(x) > 0$ for all $x \in [a, b]$. Let g be the function defined on domain $[a, b]$ by $g(x) = 1/f(x)$. If f is increasing on $[a, b]$ then g is decreasing on $[a, b]$.*

Exercise 13.15. Prove Proposition 13.16

Exercise 13.16. Prove that the function defined on the interval $[0, \infty)$ by $f(x) = \sqrt{x}$ is increasing.

Exercise 13.17. Suppose f and g are functions whose domains are subsets of the real numbers and whose targets are the set of real numbers. Suppose I and J are intervals such that $f(I) \subseteq J$ and f is increasing on I and g is increasing on J. Prove that $g \circ f$ is increasing on I.

Functions that are increasing or decreasing are always one-to-one

Proposition 13.17. *Suppose $f : I \longrightarrow \mathbb{R}$ is increasing or decreasing where the domain I is an interval.*

1. *f is one-to-one.*
2. *Let $J = \textbf{Range}(f)$. Then f has an inverse function $f^{-1} : J \longrightarrow I$.*
3. *If f is increasing then so is f^{-1} and if f is decreasing then so is f^{-1}.*

Exercise 13.18. Prove Proposition 13.17

Corollary 13.18. *For any positive integer n, the function $x \longrightarrow x^{1/n}$ is increasing. (Recall that the domain of this function is $\mathbb{R}$ if n is odd, and is $\mathbb{R}_{\geq 0}$ if n is even.)*

Proof. The function $x \longrightarrow x^n$ is increasing for all $x \in \mathbb{R}$ if n is odd, and is increasin for $x \in \mathbb{R}_{\geq 0}$ if n is even and so the inverse function inverse $x \longrightarrow x^{1/n}$ is also increasing. □

13.9 Inequalities involving lists of numbers

In Section 13.6, we used the ordered field axioms to derive various valid rules for combining two simple inequalities (each involving two quantities) by adding or multiplying them together. We want to extend these rules to apply to inequalities involving more than 2 quantities.

Proposition 13.19. *Suppose $w_1, \ldots, w_n$ and $x_1, \ldots, x_n$ are two lists of real numbers such that for all $j \in \{1, \ldots, n\}$ we have $w_j \leq x_j$. Then*

1. $\sum_{j=1}^n w_j \leq \sum_{j=1}^n x_j$.
2. *If there is at least one index j such that $w_j < x_j$ then $\sum_{j=1}^n w_j < \sum_{j=1}^n x_j$.*
3. *If all of the w_j are positive then $\prod_{j=1}^n w_j \leq \prod_{j=1}^n x_j$.*
4. *If all of the w_j are positive and there is at least one index j so that $w_j < x_j$ then $\sum_{j=1}^n w_j < \sum_{j=1}^n x_j$.*

Proof. We prove the first part and leave the second as an exercise. Suppose $w_1, \ldots, w_n$ and $x_1, \ldots, x_n$ are two lists of real numbers satisfying $w_j \leq x_j$ for all j. We prove $\sum_{j=1}^n w_j \leq \sum_{j=1}^n x_j$. We use induction on n

Case 1. Assume $n = 1$. Then the conclusion is the same as the hypothesis $w_1 \leq x_1$.

Case 2. Assume $n \geq 2$. By induction, we may assume $\sum_{i=1}^{n-1} w_i \leq \sum_{i=1}^{n-1} x_i$. Since $w_n \leq x_n$ we can apply preservation of inequality under addition, to get that $w_n + \sum_{i=1}^{n-1} w_i \leq x_n + \sum_{i=1}^{n-1} x_i$, as required.

□

Exercise 13.19. Prove the remaining parts of Proposition 13.19.

Inequalities involving the average of a list of numbers The *average* or *arithmetic mean* of a list of numbers $a_1, \ldots, a_n$, denoted $AM(a_1, \ldots, a_n)$ is given by:

$$AM(a_1, \ldots, a_n) = \frac{1}{n} \sum a_i.$$

We have the following basic inequalities:

Proposition 13.20. *For any list of numbers* $a_1, \ldots, a_n$ *we have:*

$$AM(a_1, \ldots, a_n) \geq \min(a_1, \ldots, a_n),$$

and

$$AM(a_1, \ldots, a_n) \leq \max(a_1, \ldots, a_n).$$

Proof. Suppose $a_1, \ldots, a_n$ is a list of numbers. For the first inequality, let $m = \min(a_1, \ldots, a_n)$. We have that for all $i \in \{1, \ldots, n\}$, $a_i \geq m$. Summing this inequality over i, we have $\sum_{i=1}^n a_i \geq mn$ and dividing by n we have $\frac{1}{n} \sum_{i=1}^n a_i \geq m$.

The proof of the second part is left as an exercise. □

Exercise 13.20. Prove the second part of Proposition 13.20.

Here's a more interesting inequality:

Proposition 13.21. *For any list of numbers* $a_1, \ldots, a_n$ *of real numbers, the square of the average is less than or equal to the average of the squares, that is:*

$$AM(a_1, \ldots, a_n)^2 \leq AM(a_1^2, \ldots, a_n^2).$$

Furthermore the inequality is strict unless all of the a_i *are the same.*

Proof. (of Proposition 13.21.) Suppose that $a_1, \ldots, a_n$ is a list of real numbers. It is enough to show that the difference $AM(a_1^2, \ldots, a_n^2) - AM(a_1, \ldots, a_n)^2$ is nonnegative.

$$\begin{aligned} AM(a_1^2, \ldots, a_n^2) - AM(a_1, \ldots, a_n)^2 &= \frac{1}{n} \sum_{i=1}^n a_i^2 - \frac{1}{n^2} (\sum_{i=1}^n a_i)(\sum_{i=1}^n a_i) \\ &= \frac{1}{n^2} \left(n \sum_{i=1}^n a_i^2 - (\sum_{i=1}^n \sum_{j=1}^n a_i a_j) \right). \end{aligned}$$

We will prove that this is nonnegative by relating it to the sum:

$$S = \sum_{i=1}^n \sum_{j=1}^n (a_i - a_j)^2.$$

We have:

$$\begin{aligned} S &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i^2 - 2a_ia_j + a_j^2 \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_i^2 + \sum_{i=1}^{n}\sum_{j=1}^{n} a_j^2 - 2\sum_{i=1}^{n}\sum_{j=1}^{n} a_ia_j. \end{aligned}$$

Now in the first sum, the summand (that is, the term being summed) does not depend on j, so the inner sum on j just multiplies the summand by n to get $\sum_{i=1}^{n} na_i^2$. In the second sum, the summand of the outer sum, which is $\sum_{j=1}^{n} a_j^2$ does not depend on i so the outer sum multiplies the result by n. Then by changing the index of summation to i we get that the first and second sum are the same, and together equal $2n\sum_{i=1}^{n} a_i^2$. So altogether we get:

$$S = 2n\sum_{i=1}^{n} a_i^2 - 2\sum_{i=1}^{n}\sum_{j=1}^{n} a_ia_J.$$

Notice that this is $2n^2$ times the expression we obtained for $AM(a_1^2,\ldots,a_n^2)-AM(a_1,\ldots,a_n)^2$ and so:

$$AM(a_1^2,\ldots,a_n^2) - AM(a_1,\ldots,a_n)^2 = \frac{1}{2n^2}S.$$

Since S is a sum of squares of real numbers, $S \geq 0$ and so the desired inequality is proved. Furthermore, if the a_i are not all the same then $S > 0$ and so $AM(a_1^2,\ldots,a_n^2) > AM(a_1,\ldots,a_n)^2$. □

Theorem 13.22. *Suppose that $a_1,\ldots,a_n$ and $b_1,\ldots,b_n$ are positive real numbers and that $a_1 \leq \cdots \leq a_n$ and $b_1 \leq \cdots \leq b_n$. Then $AM(a_1b_1,\ldots,a_nb_n) \geq AM(a_1,\ldots,a_n)AM(b_1,\ldots,b_n)$.*

Exercise 13.21. Prove Theorem 13.22. (Hint: Notice that in the case that $b_i = a_i$ for all i this theorem reduces to Proposition 13.21. Generalize the proof of Proposition 13.21.)

Exercise 13.22. Proof the Cauchy-Schwartz inequality, Theorem 13.10. Hint: Show that the right hand side minus the left hand side is nonnegative by relating this difference to the sum $T = \sum_{i=1}^{n}\sum_{j=1}^{n}(a_ib_i - a_jb_j)^2$.

There are two other "means" of a list of numbers that arise frequently in mathematics.

- The *geometric mean* of the list $(a_1,\ldots,a_n)$ of positive numbers is defined to be

$$GM(a_1,\ldots,a_n) = (\prod_{i=1}^{n} a_i)^{1/n}.$$

- The *harmonic mean* of the list $(a_1,\ldots,a_n)$ of positive numbers is defined by

$$HM(a_1,\ldots,a_n) = \frac{1}{\frac{1}{n}(\frac{1}{a_1} + \cdots + \frac{1}{a_n}}.$$

Thus $HM(a_1,\ldots,a_n)$ is the reciprocal of the average of the reciprocals of the a_i.

We have the following theorem:

Theorem 13.23. *For any list $a_1, \ldots, a_n$ of positive numbers,*

$$AM(a_1, \ldots, a_n \geq GM(a_1, \ldots, a_n) \qquad \text{Arithmetic-Geometric mean inequality}$$

and

$$GM(a_1, \ldots, a_n) \geq HM(a_1, \ldots, a_n) \qquad \text{Geometric-Harmonic mean inequality}$$

We will prove the arithmetic-geometric mean inequality. The geometric-harmonic mean inequality is left as an exercise.

Proof. Suppose $a_1, \ldots, a_n$ is a list of positive numbers We will show that $\frac{1}{n}\sum_{i=1}^n a_i \geq (\prod_{i=1}^n a_i)^{1/n}$. To do this we will show:

$$(\frac{1}{n}\sum_{i=1}^n a_i)^n \geq \prod_{i=1}^n a_i. \tag{7}$$

If we show this then we can take the nth root of both sides and by Corollary 13.18 the inequality is preserved and we obtain the desired inequality.

We will prove (7) by induction on n. Our induction hypothesis is: for any $1 \leq k < n$ if $b_1, \ldots, b_k$ is a list of positive numbers then $(\frac{1}{k}\sum_{i=1}^k b_i)^k \geq \prod_{i=1}^k b_i$.

Case 1. Assume $n = 1$. Then both sides of (7) are equal to a_1.

Case 2. Assume $n \geq 2$. Let $\mu = \frac{1}{n}\sum_{i=1}^n a_i$.

Our strategy will be to construct a list $b_1, \ldots, b_{n-1}$ that is very similar to $a_1, \ldots, a_n$ and has the same arithmetic mean μ. We will then use the induction hypothesis to conclude that (7) holds for the list $b_1, \ldots, b_{n-1}$. We then use this to prove that it holds for the list $a_1, \ldots, a_n$.

Let us rearrange the numbers $a_1, \ldots, a_n$ so that a_n is the largest number in the list and a_{n-1} is the smallest number on this list. By Proposition 13.20 we have $a_n \geq \mu$ and $a_{n-1} \leq \mu$. (**Comment**: At this point in the proof, the reason for rearranging the numbers in this way will probably seem mysterious. The reason for doing this will only become clear later in the proof.)

Now define the list $b_1, \ldots, b_{n-1}$ by defining $b_i = a_i$ for $i \leq n-2$ and $b_{n-1} = a_{n-1} + a_n - \mu$. We claim that the arithmetic mean of this list is μ.

Exercise 13.23. Prove that the arithmetic mean of $b_1, \ldots, b_{n-1}$ is μ.

Also, all the terms in the list are positive since $b_i = a_i > 0$ for $i \leq n-2$ and $b_{n-1} = a_{n-1} + (a_n - \mu) \geq a_{n-1} > 0$.

So by induction we have:

$$\mu^{n-1} \geq \prod_{i=1}^{n-1} b_i = (\prod_{i=1}^{n-2} a_i) \times (a_{n-1} + a_n - \mu)$$

We multiply both sides of this inequality by $(a_{n-1} \times a_n)/(a_{n-1} + a_n - \mu)$ to get:

$$\mu^{n-1} \times \frac{a_{n-1}a_n}{a_{n-1} + a_n - \mu} \geq \prod_{i=1}^{n} a_i.$$

To complete the proof, we show that the lefthand side of the inequality is at most μ^n (and then by transitivity we will have $\mu^n \geq \prod_{i=1}^{n} a_i$.) To do this we show

$$\mu \geq \frac{a_{n-1}a_n}{a_{n-1} + a_n - \mu},$$

and then multiply both sides by μ^{n-1}.

We will deduce this last inequality from the following inequality $\mu(a_{n-1}+a_n-\mu)-a_{n-1}a_n \geq 0$. This inequality holds because the lefthand side is equal to $(\mu-a_{n-1})(a_n-\mu)$ which is nonnegative since $\mu \geq a_{n-1}$ and $a_n \geq \mu$. (This is why we rearranged the list earlier in the proof.) Therefore $\mu(a_{n-1} + a_n - \mu) - a_{n-1}a_n \geq 0$ and adding $a_{n-1}a_n$ to both sides and dividing both sides by $a_{n-1} + a_n - \mu$ yields the required inequality.

□

Exercise 13.24. Prove that the geometric-harmonic mean inequality follows from the arithmetic-geometric mean inequality. That is, give a proof of the geometric-harmonic mean inequality where you are are allowed to assume that the arithmetic-geometric mean inequality is true.

Exercise 13.25. For any real numbers x and y and any even positive integer k, prove that $\sum_{i=0}^{k} x^i y^{k-i} \geq 0$.