10 Basic proofs involving real numbers [11]

In this chapter we begin the systematic study of the *real number system.* This is the familiar system of numbers 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 (and some later ones) you'll learn *how to prove* universal principles about real numbers.

The usual approach for such a systematic study is to start with a small number of elementary definitions and principles (called *axioms*), and use these to prove everything. The drawback to this approach is that it requires that we start off doing many tedious proofs that are very elementary in order to build up many basic facts. We will follow a *modified axiomatic approach*; we'll state a collection of general principles that we'll use in our proofs. This collection of principles is larger than the usual set of axioms, and helps us avoid spending too much time proving very easy results.

The real number system consists of the set $\mathbb{R}$ of real numbers, together with two binary operations, addition ($+$) and multiplication ($\times$ or $\cdot$). The set $\mathbb{R}$ has two special elements named 0 and 1.

The basic properties of the real numbers include (1) Algebraic properties, which are properties involving equations, and (2) Properties of inequalities. There is one additional property of the set of real numbers, which we call the *betweenness property* which corresponds to the intuitive idea that there are "no gaps" in the real number line.

10.1 Algebraic properties of the real numbers

The algebraic properties are themselves divided into various groups.

Closure properties of addition and multiplication

- $\mathbb{R}$ *is closed under addition.* The sum of two real numbers is a real number.
- $\mathbb{R}$ *is closed under multiplication.* The product of two real numbers is a real number

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 real numbers x and y, $x + y = y + x$.
- *Associative Property of Addition.* For all real numbers x, y and z, $(x+y)+z = x+(y+z)$.
- Commutative Property of Multiplication. For all real numbers x and y, $xy = yx$.
- Associative Property of Multiplication. For all real numbers x, y and z, $x(yz) = (xy)z$.

[11] Version 4/3/15.

- Distributive Property of Multiplication over Addition.For all real numbers x,y and z, $x(y+z) = xy + xz$.

Axioms of 0 and 1

- *Axiom of 0.* There is a special element of $\mathbb{R}$ called 0, with the property that for every $x \in \mathbb{R}$, $x + 0 = x$. The element 0 is called the *additive identity elements* of $\mathbb{R}$.
- *Axiom of 1.* There is a special element of $\mathbb{R}$ called 1, with the property that for every $x \in \mathbb{R}$, $x \cdot 1 = x$. The element 1 is called the *multiplicative identity element* of $\mathbb{R}$.

Additive and multiplicative inverse axioms For a real number x, 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 real number $x \in \mathbb{R}$ has a unique additive inverse, which is denoted $-x$. The additive inverse of x is equal to $(-1)x$.
- *Multiplicative inverse axiom* Every nonzero real number $x \in \mathbb{R}$ has a unique multiplicative inverse which is denoted $\frac{1}{x}$.

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* $\frac{x}{y}$ is defined to mean $x \cdot \frac{1}{y}$, which is the sum of x and the multiplicative inverse of y.

Algebraic Manipulation Since elementary school, you've learned how to use 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 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".

10.2 Order properties of the real numbers

The most important way to compare two real numbers is 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 10.1. *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.

The tripartition of the real numbers The set of three real numbers is partitioned into two sets, the singleton set $\{0\}$, the set $\mathbb{R}_+$ *positive real numbers* and the set $\mathbb{R}_-$ of *negative real numbers.* A number is *nonnegative* if it is positive or 0 and is nonpositive if it is negative or 0. *Basic Properties of Positive and Negative numbers*

- The sum of any list of positive numbers is positive.
- The sum of any list of negative numbers is negative.
- The product of two nonzero numbers is positive if both are positive or both are negative, and is negative otherwise.
- The produce of a list of numbers is positive if the number of negative numbers in the list is even, and is negative if the number of negative numbers in the list is odd.
-
- For all positive numbers x, $-x$ is negative. (Recall that $-x$ is the unique number such that $x + (-x) = 0$, and is equal to $(-1)x$.

Corollary 10.2. *The square of any real number is positive.*

Definition of $<$ and $\leq$ We can use the notion of positive and negative to define:

- $x < y$ means that $y - x$ is positive.
- $x \leq y$ means that $y - x$ is nonnegative.
- $x > y$ means that $x - y$ is positive.
- $x \geq y$ means that $x - y$ is nonnegative.

The basic properties of positive and negative numbers can be used to show:

Proposition 10.3. *For any real numbers x, y, z the following hold:*

1. *Exactly one of $x < y$, $x = y$ and $y < x$ holds.*

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

Proof. Suppose w, x, y and z are arbitrary real numbers.
Proof of (1). Assume first that $x = y$. Then $y - x = x - y = 0$ and so neither $y - x$ nor $x - y$ is positive and so $x \not< y$ and $y \not< x$.

Now assume $x \neq y$. Then $y - x \neq 0$ and so is positive or negative. If it is positive, then by definition $y > x$ and also $x - y = -(y - x)$ must be negative and so $y \not< x$. Similarly, if $y - x$ is negative, then $x \not< y$, and also $x - y = -(y - x)$ is positive, so $y < x$.
Proof of 2. Assume $x < y$ and $y < z$. Then $y - x$ and $z - y$ are positive so $(z - y) + (y - x) = z - x$ is positive. Therefore $x < z$. □

Proposition 10.4. *For any real numbers $w_1, \ldots, w_n$ and $x_1, \ldots, x_n$, if for all $j \in \{1, \ldots, n\}$ we have $w_j \leq x_j$, then $\sum_{j=1}^{n} w_j \leq \sum_{j=1}^{n} x_j$.*

Exercise 10.1. Proof Proposition 10.4.

Proposition 10.5. *Suppose that x, y, z, w are arbitrary real numbers.*

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

2. *If $w \leq x$ and $y \leq z$ and $w \geq 0$ and $y \geq 0$ then $wy \leq xz$.*

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

Proof. Proof of 1. 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 10.2. Prove the remaining parts of Proposition 10.3.

10.3 The completeness axiom

The axioms that we've presented so far for the real numbers fall into two groups: the algebraic axioms, and inequality 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 10.1. (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. However, no one knows how to prove this assertion from the algebraic axioms and inequality axioms alone.

In fact, as we'll see: It is *impossible* to prove the square root principle from the algebraic axioms and the inequality axioms.

How can we know that it is impossible to prove the square root principle with just the algebraic and inequality 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 inequality axioms. It's another thing to say that it's *not possible* to do this. How can we know such a thing?

It turns out that this is something that can be proved. The proof would require us to carefully discuss and develop ideas from the field of mathematical logic. Since mathematical logic is not our main subject, we will not do that here. Instead, we'll explain informally (without proof) the main idea that is used to prove that it is impossible to prove the square root principle form the algebraic and inequality axioms.

Recall that $\mathbb{Q}$ denotes the set of all rational numbers. (Recall that a number is said to be rational if it can be written as the ratio of two integers.) The set $\mathbb{Q}$ is a subset of $\mathbb{R}$.

The algebraic axioms include the closure properties: that the sum of two real numbers is a real number and the product of two real numbers is a real number. It is also true that the sum of two rational numbers is rational, and the product of rational numbers is rational. Also, the additive inverse of a rational number is rational and the multiplicative inverse of a rational number is rational. When we replace $\mathbb{R}$ by $\mathbb{Q}$, we get a new set of principles: the algebraic and inequality axioms for the set $\mathbb{Q}$. If you go through all of these new principles you can check the following:

Observation 1. All of the algebraic and inequality axioms for $\mathbb{Q}$ are true.

Now suppose that we could prove the square root principle for $\mathbb{R}$ from the algebraic and inequality axioms for $\mathbb{R}$. Now instead of starting from the algebraic and inequality axioms for the reals, we start from the algebraic and inequality axioms for $\mathbb{Q}$. Then following the same proof we'd be able to prove:

Assertion 10.2. (Square root principle for $\mathbb{Q}$) For every $x \in \mathbb{Q}$, if $x > 0$ there is a positive number $z \in \mathbb{Q}$ such that $z^2 = x$. In other words, every positive real number has a positive square root.

But there's a problem:

Observation 2. The square root principle for $\mathbb{Q}$ is not true!

We'll see why this is the case 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 for $\mathbb{R}$ from the algebraic and inequality axioms, then a similar proof could be used to prove the square root principle for $\mathbb{Q}$. So we 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 10.3. Prove that the product of any two odd numbers is odd.

Theorem 10.6. *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, we must have that a is divisible by 2. 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 have b is even. But then a and b have a common factor of 2, which is a contradiction. 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. $\square$

So Observations 1 and 2 together lead to the conclusion that the algebraic and inequality axioms are not enough to prove the square root principle. So we need at least one more axiom. It turns out that we'll just need one axiom. This axiom is called the *completeness axiom*. There are different ways to formulate the axiom. Here we'll give a formulation that is a bit more intuitive than the usual formulation.

We need the following definitions. Suppose that A and B are sets of real numbers and z is a real number. We write $A \leq z$ if for every $x \in A$ we have $x \leq z$. Also we write $A \leq B$ if for all $x \in A$ and $y \in B$ we have $x \leq y$.

> **The Completeness Axiom.** Suppose that A and B are subset of $\mathbb{R}$ satisfying $A \leq B$. Then there is a real number z satisfying $A \leq z$ and $z \leq B$. We say that z *lies between A and B*.
>
> **Exercise 10.4.** If A is the empty set what does $A \leq z$ imply about z, and what does $A \geq z$ imply about z?

As mentioned, there are other ways to formulate the completeness axiom; we may see some of these later. We'll refer to the above as the *betweenness version of the completeness axiom.*

Let's see how the completeness axiom is used to prove the square root principle. However, for simplicity, we won't prove the full square root principle.

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

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

Claim: $A \leq B$.

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

Since $A \leq B$, the Completeness Axiom tells us that there is a number we'll call z such that $A \leq z \leq B$. We want to show that $z^2 = x$, which will complete the proof.

We first want to show that $z > 0$. We know that $z \geq A$ and A contains only positive numbers, so we'd like to say that $z > 0$. But if A happens to be empty then $z \geq A$ is vacuously true, and we can't conclude that $z > 0$. So we need to show that A is nonempty. This is easy: if $x \geq 1$ then $1/2 \in A$. If $x < 1$ then $x^2 < x$, so $x \in A$. In either case A is nonempty, so $z > 0$.

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

Case 1. Assume $z^2 < x$. Then since $z > 0$ we have that $z \in A$. We'll now show that there is a number $\delta > 0$ such that $z + \delta \in A$, which is a contradiction to $z \geq A$. Define the function $g(y) = x - (z+y)^2$. Then $z + y \in A$ if and only if $g(y) > 0$, so we must find a number $\delta > 0$ such that $g(\delta) > 0$. Observe that $g(y) = (x - z^2) - 2zy - y^2$. If $y \in (0,1)$ then

$$g(y) > x - z^2 - 2zy - y = (x - z^2) - y(2z+1).$$

Now choose $\delta = (x - z^2)/(2z + 1 + x)$. We note that δ is positive, since it is the ratio of positive numbers. Also $\delta < 1$ since $x - z^2 < x + 2z + 1$ (since $z > 0$). Therefore,

$$\begin{aligned}
g(\delta) &> (x - z^2) - \delta(2z+1) \\
&= (x - z^2) - \frac{x - z^2}{2z + 1 + x}(2z+1) \\
&= (x - z^2)(1 - \frac{2z+1}{2z+1+x}),
\end{aligned}$$

which is positive since $x > z^2$ and $1 - (2z+1)/(2z+1+x)$ is positive.

So we have found a positive δ such that $g(\delta) > 0$ and therefore $z + \delta \in A$, contradicting that $A \leq z$. Therefore $z \notin A$.

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

Exercise 10.5. Show that case 2 leads to a contradiction.

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

10.4 Summations and Products

Suppose I is any finite set, and $(a_i : i \in I)$ is an indexed collection of real numbers.

- $\sum_{i \in I} a_i$, 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.

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:

$$\sum_{i=m}^{n} a_i = \sum_{i\in I} a_i$$
$$\prod_{i=m}^{n} a_i = \prod_{i\in I} a_i.$$

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 10.7. *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 10.8. *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 substitition* 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 10.1. 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 10.9. *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 10.6. Give an alternate proof using dot-dot-dot notation and telescoping sums.

10.5 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 10.10. *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 10.7. Prove the second part of Proposition 10.10.

Here's a more interesting inequality:

Proposition 10.11. *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 10.11.) Suppose that $a_1, \dots, a_n$ is a list of real numbers. It is enough to show that the difference $AM(a_1^2, \dots, a_n^2) - AM(a_1, \dots, a_n)^2$ is nonnegative.

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

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:

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

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 $\sum_{i=1}^{n} n a_i^2$. 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:

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

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

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

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 $AM(a_1^2, \dots, a_n^2) > AM(a_1, \dots, a_n)^2$. □

Theorem 10.12. *Suppose that $a_1, \dots, a_n$ and $b_1, \dots, b_n$ are positive real numbers and that $a_1 \leq \cdots \leq a_n$ and $b_1 \leq \cdots \leq b_n$. Then $AM(a_1 b_1, \dots, a_n b_n) \geq AM(a_1, \dots, a_n)AM(b_1, \dots, b_n)$.*

Exercise 10.8. Prove Theorem 10.12. (Hint: Notice that in the case that $b_i = a_i$ for all i this theorem reduces to Proposition 10.11. Generalize the proof of Proposition 10.11.)

Exercise 10.9. Proof the Cauchy-Schwartz inequality, Theorem 10.1. Hint: Show that the right hand side minus the left hand side is nonnegative by relating this difference to the sum $T = \sum_{i=1}^n \sum_{j=1}^n (a_i b_i - a_j b_j)^2$.

There are two other "averages" 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 to be $HM(a_1, \ldots, a_n) = \frac{1}{\frac{1}{n}(a_1 + \cdots + a_n)}$.

We have the following theorem:

Theorem 10.13. *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

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

The easiest proofs of these results use calculus; but we're not ready to look at proofs using calculus yet. In a later section, we'll show how to prove the arithmetic-geometric mean inequality using the principle of mathematical induction.

Exercise 10.10. 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 10.11. For any real numbers x and y and any even positive integer k, prove that $\sum_{i=0}^k x^i y^{k-i} \geq 0$. (Hint: Show that this sum can be rewritten as a sum of squares.)

10.6 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 10.2. 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 10.14. *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 10.12. Prove Theorem 10.14.

Proposition 10.15. *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 10.13. Prove Proposition 10.15

Exercise 10.14. Prove that the function defined on the interval $[0, \infty)$ by $f(x) = \sqrt{x}$ is increasing.

Exercise 10.15. 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.