MATH 117 Notes Jan. 8 2026 (Draft)

Given an ordered field S, we can prove the following statements:

1. $a < b \iff -a > -b$.

$$\begin{aligned} & a < b \\ \implies & a + (-a - b) < b + (-a - b) \\ \implies & -b < -a \end{aligned}$$

$$\begin{aligned} & -a > -b \\ \implies & -a + (a + b) > -b + (a + b) \\ \implies & b > a \blacksquare \end{aligned}$$

2. If $a \neq 0$, then $a^2 > 0$.

$$\begin{aligned} & a > 0 \\ \implies & a \cdot a > 0 \cdot a \\ \implies & a^2 > 0 \end{aligned}$$

$$\begin{aligned} & a < 0 \\ \implies & -a > 0 \\ \implies & (-a) \cdot (-a) > 0 \cdot (-a) \\ \implies & a^2 > 0 \blacksquare \end{aligned}$$

3. If $a > b > 0$ and $c > d > 0$, then $ac > bd$.

$$\begin{gathered} ac > bc \\ bc > bd \\ \therefore ac > bd \blacksquare \end{gathered}$$

Exercise. Given an ordered field S, prove that if $a \in S$, then $a^{-1} > 0$.

Remark. In any ordered field, $1 > 0 \implies 1 + 1 > 0 + 1$. Inductively,

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} > \underbrace{1 + 1 + \cdots + 1}_{n-1 \text{ times}}$$

Therefore, an ordered field is not finite. Note as well that $n > n - 1$.

The AGM Inequality

Proposition. Suppose that, in an ordered field, $a_1, a_2, \ldots, a_n$ are all greater than zero and *not all equal.* Then,

$$a_1 a_2 \cdots a_n < \left(\frac{a_1 + a_2 + \cdots + a_n}{n}\right)^n.$$

Note that, for the elements $a_1, a_2, \ldots, a_n$, the expression $\frac{a_1 + a_2 + \cdots + a_n}{n}$ is the **arithmetic mean**, and $(a_1 a_2 \cdots a)^{\frac{1}{n}}$ is the **geometric mean**. Thus, this proposition is named for the 'arithmetic-geometric mean inequality.'

Proof

Consider the case when $n = 2$. If $a_1 \neq a_2$, then $a_1 - a_2 \neq 0$. It follows that $(a_1 - a_2)^2 > 0$. With some manipulation, we arrive at

$$a_1 a_2 < \left(\frac{a_1 + a_2}{2}\right)^2.$$

Hence, the proposition is true for $n = 2$.

Now, assume the proposition is true for some n terms. Suppose that $a_1, a_2, ..., a_{2n}$ are given such that $a_1 \neq a_2$ and $a_i > 0$ for every i. Then, by the hypothesis,

$$\begin{aligned} a_1 a_2 \cdots a_n &< \left(\frac{a_1 + a_2 + \cdots + a_n}{n}\right)^n \\ a_{n+1} a_{n+2} \cdots a_{2n} &\leq \left(\frac{a_{n+1} + a_{n+2} + \cdots + a_{2n}}{n}\right)^n \end{aligned}$$

Multiplying these two inequalities together:

$$\begin{aligned} a_1 a_2 \cdots a_n &< \left(\left(\frac{a_1 + a_2 + \cdots + a_n}{n}\right) \cdot \left(\frac{a_{n+1} + a_{n+2} + \cdots + a_{2n}}{n}\right)\right)^n \\ &< \left(\frac{a_1 + a_2 + \cdots + a_{2n}}{2n}\right)^{2n} \quad \text{by the } n = 2 \text{ case} \end{aligned}$$

Hence, it follows by induction that the proposition is true for all integers of the form $n = 2^m$. For integers not of this form, we proceed as follows.

Choose m such that $2^m > n$. Let $A = (a_1 + a_2 + \cdots + a_n)/n$. Then,

$$\begin{aligned} a_1 a_2 \cdots a_n \cdot A^{2^m - n} &< \left(\frac{a_1 + a_2 + \cdots + a_n + (2^m - n)A}{2^m}\right)^{2^m} \\ &= \left(\frac{nA + (2^m - n)A}{2^m}\right)^{2^m} \\ &= A^{2^m} \end{aligned}$$

Now, multiplying both sides by $\left(A^{2^m - n}\right)^{-1}$, we obtain $a_1 a_2 \cdots a_n < A^n$ as required. ■

Motivation for the real numbers

To obtain $\mathbb{R}$, we want the axioms of ordered fields plus one more: the **least upper bound axiom**.

Lemma. There is no $x \in \mathbb{Q}$ such that $x^2 = 2$.

Proof. Suppose $p/q \in \mathbb{Q}$ where $p^2/q^2 = 2$, $q > 0$, and p and q have no common factors.

Then $p^2 = 2q^2$. Therefore, $2 \mid p^2$ and so $2 \mid p$. By definition, $p = 2p'$ for some $p' \in \mathbb{Z}$.

By substitution, we get $2(p')^2 = q^2$, so $2 \mid q^2$ and thus $2 \mid q$. Hence, 2 divides both p and q, a contradiction. Therefore, there is no $x \in \mathbb{Q}$ for which $x^2 = 2$. ■

Bounds

Let S be an ordered set that satisfies axioms B1-B4.

A non-empty subset $A \subseteq S$ is **bounded above** if there is a $b \in S$ such that $b \geq a$ for every $a \in A$. The element b is called an **upper bound** of A.

A is **bounded below** if there is a $b' \in S$ such that $b' \leq a$ for every $a \in A$. We say that b is a **lower bound** of A.

If A is both bounded above and bounded below, we say that A is **bounded**.

For example, the set of even integers is not bounded above nor below. However, the set of negative integers is bounded above by any number greater or equal to -1.

Least upper bound

Our last axiom, C, is known as the **least upper bound** or **completeness** axiom. An ordered set S satisfies C if any non-empty subset $A \subseteq S$ bounded above has a least upper bound.

Symbolically, S satisfies C if there is a $b \in S$ such that $b \geq a$ for every $a \in A$; and, if there is another $b' \in S$ for which $b' \geq a$ for every $a \in A$, then $b' \geq b$. We call b the **least upper bound** of A. It is also known as the **supremum** of A.

We may notate b as $\operatorname{lub}(A)$, $\sup(A)$, or $\sup_a(a \in A)$.

As an example, $\mathbb{Z}$ satisfies the axiom, but $\mathbb{Q}$ does not. For example, take $A \subseteq \mathbb{Q}$ where $A = \{a \in \mathbb{Q} \mid a^2 < 2\}$. Recall that no rational number q satisfies $q^2 = 2$. Since it is also impossible to find the 'next' rational number, the set A has no least upper bound.

Constructing the reals

The set of real numbers $\mathbb{R}$ is an ordered field that satisfies the least upper bound axiom. That is, $\mathbb{R}$ satisfies axioms A1-A11, B1-B4, and C.

Assertion. The real numbers exist – they can be constructed from $\mathbb{Q}$, which in turn comes from $\mathbb{Z}$. In a sense, the reals are a *completion* of $\mathbb{Q}$.