

Math 351 Notes

Instructor Arkady Etkin

The Real Number System

- **Proposition:**

Let p be a prime number. Then there are no integers $m, n \in \mathbb{Z}$ such that $(\frac{m}{n})^2 = p$.

Proof:

Suppose that such a number does in fact exist. That is, suppose that there is a rational fraction $\frac{m}{n}$ such that $(\frac{m}{n})^2 = p$. We can assume that this fraction is in simplest terms, i.e. $\gcd(m, n) = 1$, since otherwise we could just divide by the common factor and get an equivalent fraction.

Then the equation above can be written as $m^2 = n^2 p$, which means that $p \mid m^2$ (p divides m^2). Thus, it follows that $p \mid m$. In particular, there exists an integer k such that $m = k p$, from which it follows that

$$m^2 = k^2 p^2 = n^2 p \implies k^2 p = n^2$$

But this means that $p \mid n^2$ and therefore that $p \mid n$. ($\implies \Leftarrow$)

This is a contradiction, because $1 = \gcd(m, n) \geq p > 1$. Thus, we conclude that no rational function $x^2 = p$ exists. ■

Observation:

Let p be a prime number, and set $A = \{r \in \mathbb{Q}^+ : r^2 < p\}$ and $B = \{r \in \mathbb{Q}^+ : r^2 > p\}$. Then for each $r \in A$ there exists $s \in A$, such that $r < s$. Similarly, for each $r \in B$ there exists $s \in B$, such that $s < r$.

Let's define this number s :

\Leftarrow If $r \in A$, then

$$\begin{aligned} r^2 < p &\implies r < \sqrt{p} = r + (\sqrt{p} - r) \\ &= r + (\sqrt{p} - r) \cdot \frac{(\sqrt{p} + r)}{(\sqrt{p} + r)} \end{aligned}$$

$$= r + \frac{p-r^2}{\sqrt{p+r}} > \frac{r + \frac{p-r^2}{p+r}}{\text{we call this number } s} > r$$

↔ Similarly, if $r \in B$, we have

$$\begin{aligned} r^2 > p &\implies r > \sqrt{p} = r - (r - \sqrt{p}) \\ &= r - (r - \sqrt{p}) \cdot \frac{(r + \sqrt{p})}{(r + \sqrt{p})} \\ &= r - \frac{r^2 - p}{r + \sqrt{p}} < \frac{r - \frac{r^2 - p}{r + p}}{\text{we call this number } s} < r \end{aligned}$$

Then $s \in \mathbb{Q}^+$. If $r \in A$, then $r^2 - p < 0$, implying that $r < s$. On the other hand, if $r \in B$, then $r^2 - p > 0$, implying that $r > s$.

Note: The observation above suggests that any element in $B \subset \mathbb{Q}$ is an upper bound of A . In other words, if $s \in B$ and $r \in A$, then $r < s$.

Furthermore A has no smallest upper bound (in \mathbb{R}):

For any $s \in B$, there is an $s_1 < s$, with $s_1 \in B$, such that s_1 is an upper bound of A . Similar reasoning shows that B is bounded below by elements in A with no largest lower bound. We will soon examine this observation more closely.

Definition: Let S be a set. An order on S is a relation, denoted by $<$, with the following two properties:

(i) If $x, y \in S$, then one and only one of the statements below is true :

$$x < y, \quad x = y, \quad y < x$$

(ii) Let $x, y, z \in S$. Then if $x < y$ and $y < z$, it is always true that $x < z$.

Definition: An ordered set is a set S in which an order k is defined. For example, \mathbb{Q} is an ordered set if $r < s$ is defined to mean that $s - r$ is a positive rational number.

Definition: Suppose S is an ordered set, and $E \subset S$. If there exists a $\beta \in S$ such that $x \leq \beta$ for every $x \in E$, then we say that E is bounded above, and call β an **upper bound** of E . **Lower bounds** are defined in the same way (with \geq in place of \leq).

Definition: Suppose S is an ordered set, $E \subset S$, and E is bounded above. Moreover, suppose there exists an $\alpha \in S$ with the following properties:

(i) α is an upper bound of E .

(ii) If $\gamma < \alpha$, then γ is not an upper bound of E .

Then α is called the **least upper bound** or **supremum** of E , denoted $\alpha = \sup(E)$.


The **greatest lower bound**, or **infimum**, of a set E which is bounded below is defined in the same manner. The statement $\alpha = \inf(E)$ means that α is a lower bound of E and that no β with $\beta > \alpha$ is a lower bound of E .

Example:

a) Consider the sets A and B described above as subsets of the ordered set \mathbb{Q} . The set A is bounded above. In fact, the upper bounds of A are exactly the members of B . Since B contains no smallest member, A has no least upper bound in \mathbb{Q} . Similarly, B is bounded below: the set of all lower bounds of B consists of A and of all $r \in \mathbb{Q}$ with $r \leq 0$. Since A has no largest member, B has no greatest lower bound in \mathbb{Q} .

b) If $\alpha = \sup(E)$ exists, then α may or may not be a member of E . For instance, let E_1 be the set of all $r \in \mathbb{Q}$ with $r < 0$. Let E_2 be the set of all $r \in \mathbb{Q}$ with $r \leq 0$. Then $\sup(E_1) = \sup(E_2) = 0$ with $0 \notin E_1$ and $0 \in E_2$.

c) Let E consist of all numbers $1/n$, where $n = 1, 2, 3, \dots$

Then $\sup(E) = 1$, which is in E , and $\inf(E) = 0$, which is not in E . 

Definition: An ordered set S is said to have the least upper bound property if the following is true: If $E \subset S$ is not empty, and E is bounded above, then $\sup(E)$ exists in S . **

Note: Observe that \mathbb{Q} does not have the least upper bound property. **

We now show that every set S with the least upper bound property also has the greatest lower bound property.

• Theorem:

Suppose S is an ordered set with the least upper bound property and let $B \subset S$ be nonempty and bounded below. In addition, let L be the set of all lower bounds of B . Then $\alpha = \sup(L)$ exists in S and $\alpha = \inf(B)$. In particular, $\inf(B)$ exists in S .

Proof:

Since B is bounded below, L is nonempty. Since L consists of exactly those $y \in S$ which satisfy the inequality $y \leq x \ \forall x \in B$, we see that every $x \in B$ is an upper bound of L .

Then L is bounded above.

Our hypothesis about S implies therefore that L has a supremum in S , call it α . If $\gamma < \alpha$, then γ is not an upper bound of L . In particular, there is some $\beta \in L$ such that $\gamma < \beta$, implying that γ is a lower bound of B . Thus $\alpha \leq x \ \forall x \in B$. It follows that $\alpha \in L$. If $\alpha < \lambda$, then $\lambda \notin L$, since α is an upper bound of L .

Thus we have shown that $\alpha \in L$ but $\lambda \notin L$ if $\alpha < \lambda$. In other words, α is a lower bound of B but λ is not if $\lambda > \alpha$. This implies that $\alpha = \inf(B)$. ■

- **Existence Theorem:**

There exists an ordered field \mathbb{R} which has the least upper bound property. Moreover, \mathbb{R} contains \mathbb{Q} as a subfield.

Proof: (On Rudin's, chapter 1 appendix) ■

We now derive some important properties of the field \mathbb{R} .

- **Axiom of Completeness:**

Every nonempty set of real numbers that is bounded above has a least upper bound.

- **Theorem:**

a) If $x, y \in \mathbb{R}$, and $x > 0$, then there is a positive integer n such that $n x > y$.

b) If $x, y \in \mathbb{R}$, and $x < y$, then there exists a $p \in \mathbb{Q}$ such that $x < p < y$.

**Note: Part a) is usually referred to as the archimedean property of \mathbb{R} . Part b) may be stated by saying that \mathbb{Q} is dense in \mathbb{R} : Between any two real numbers there is a rational one. **

Proof:

a) Set $A = \{n x : n \in \mathbb{N}\}$. Now let's assume that a) is false, so that y is an upper bound of A , and define $\alpha = \sup(A)$. We have that $x > 0$, which implies that $\alpha - x < \alpha$, and this in turn means that $\alpha - x$ is not an upper bound of A .

Hence $\alpha - x < m x$ for some positive integer m . But then $\alpha < (m + 1) x \in A$, which contradicts the statement that $\alpha = \sup(A)$. ($\Rightarrow \Leftarrow$)

Therefore A is not bounded above. ✓

b) Since $x < y$, we have $y - x > 0$. From a), we conclude that there is an integer $n > 0$ such that $n(y - x) > 1$. Observe that, for some integer m , we have $m - 1 \leq n x < m$.

Observe also that $m \leq 1 + n x < n y$.

Thus, since $nx < m$, we have $nx < m < ny$. In particular, $x < \frac{m}{n} < y$. This proves b), with $p = \frac{m}{n}$. ✓ ■

Now we are ready to prove the existence of n^{th} roots of positive reals.

• **Theorem:**

For every real $x > 0$ and every integer $n > 0$, there is one and only one real y such that $y^n = x$.

Proof:

That there is at most one such y is clear, since if there was another y_1 , then we would have $y < y_1$, which implies that $y^n < y_1^n$ or $y_1 < y$ which implies that $y_1^n < y^n$.

Let E be the set consisting of all positive real numbers t such that $t^n < x$, i.e.

$E = \{t \in \mathbb{R}^+ : t^n < x\}$, with $x \in \mathbb{R}$. We first need to show that E is not empty.

If we let $t = \frac{x}{1+x}$, then $0 \leq t < 1$. Hence $t^n \leq t < x$, which means that $t \in E$, thus E is not empty.

If $t > 1+x$, then $t^n \geq t > x$, so that $t \notin E$. Thus $1+x$ is an upper bound of E .

Hence, the existence theorem implies that there exists an element y such that $y = \sup(E)$.

We initially set out to prove that $y^n = x$. To show that this is true, we must now show that the inequalities $y^n < x$ and $y^n > x$ yield a contradiction.

The identity

$$b^n - a^n = (b - a)(b^{n-1} + b^{n-2}a + b^{n-3}a^2 + \dots + a^{n-1})$$

yields the inequality

$$b^n - a^n < (b - a)(b^{n-1} + b^{n-1} + \dots + b^{n-1}) = (b - a)n b^{n-1}.$$

So

$$b^n - a^n < (b - a)n b^{n-1}$$

when $0 < a < b$.

We are now going to use this identity.

Let $b > a > 0$ and set $h = b - a$. So $0 < h < 1$ and

$$h < \frac{x - y^n}{n(y+1)^{n-1}}$$

Put $a = y$, $b = y + h$. Then

$$(y + h)^n - y^n < h n (y + h)^{n-1} < h n (y + 1)^{n-1} < x - y^n.$$

Thus $(y + h)^n < x$, and $y + h \in E$. Since $y + h > y$, this contradicts the fact that y is an

upper bound of E .

Assume that $y^n > x$ and then set

$$k = \frac{y^n - x}{n y^{n-1}}$$

Clearly $k > 0$. Observe that $n k = \frac{y^n - x}{y^{n-1}} < \frac{y^n}{y^{n-1}} = y$.

In particular, $0 < k < y$.

Thus,

$$y^n - (y - k)^n < k n y^{n-1} = y^n - x.$$

In particular,

$$x < (y - k)^n.$$

It follows that $y - k$ is an upper bound of E .

But $y - k < y$, which contradicts the fact that y is the least upper bound of E .

Hence, $y^n = x$, as we set out to prove. ■

(Alternate) Proof:

Let E be defined as before. Follow the argument of the proof above to show that E is not empty and bounded above. Then set $y = \sup(E)$.

We will show that $y^n = x$ by proving that $|y^n - x| < \epsilon$ for any $\epsilon > 0$. This will imply that $|y^n - x| = 0$ or $y^n = x$.

Let $h > 0$. If $h < y$, then $y - h$ is a positive number that is not an upper bound of E . In particular, there is some $t \in E$ such that $y - h < t < y$ and therefore

$$(y - h)^n < t^n < x.$$

Thus, $y - h \in E$.

Observe now that $(y + h)^n > x$, for if $(y + h)^n \leq x$, then $(y + \frac{h}{2})^n < (y + h)^n \leq x$ implying that $y + \frac{h}{2} \in E$ and contradicting the fact that y is an upper bound of E .

It follows that $(y - h)^n < x < (y + h)^n$. Naturally, $(y - h)^n < y^n < (y + h)^n$.

Geometrically, the distance from y^n to x , $|y^n - x|$, is less than $(y + h)^n - (y - h)^n$. This can be proven analytically without much difficulty.

Thus,

$$|y^n - x| < (y + h)^n - (y - h)^n = 2 \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2i+1} y^{n-2i-1} h^{2i+1}$$

$$< 2h \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2i+1} y^{n-2i-1}$$

The expression

$$2 \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2i+1} y^{n-2i-1} h^{2i}$$

was derived from expanding $(y+h)^n - (y-h)^n$ with the help of the binomial theorem. The last inequality was derived from the assumption that h may be selected to be less than 1.

Notice that $B = 2 \sum_{i=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2i+1} y^{n-2i-1}$ is just a number and $hB < \epsilon$ for any ϵ given a sufficiently small h . Thus, $|y^n - x| < \epsilon$ as desired. ■

• **Corollary:**

If a and b are positive real numbers and n is a positive integer, then

$$(ab)^{1/n} = a^{1/n} b^{1/n}$$

Proof:

Let $\alpha = a^{1/n}$ and $\beta = b^{1/n}$. Then

$$a b = \alpha^n \beta^n = (\alpha \beta)^n,$$

since multiplication is commutative. The uniqueness assertion of the theorem to which this is a corollary shows that

$$(ab)^{1/n} = \alpha \beta = a^{1/n} b^{1/n}. \quad \blacksquare$$

One approach to describe the elements of \mathbb{R} is by using decimals. The following propositions give some insight.

• **Proposition:**

Fix an integer $p \geq 2$ and let $\{a_n\}$ be any sequence of integers satisfying $0 \leq a_n \leq p-1$ for

all n . Then, $\sum_{n=1}^{\infty} \frac{a_n}{p^n}$ converges to a number in $[0, 1]$.

Proof:

Since $a_n \geq 0$, the partial sums $\sum_{n=1}^N \frac{a_n}{p^n}$ are nonnegative and increase with N . Thus, to show

that the series converges to some number in $[0, 1]$, we just need to show that 1 is an upper bound for the sequence of partial sums.

But this is easy:

$$\sum_{n=1}^N \frac{a_n}{p^n} \leq \sum_{n=1}^N \frac{p-1}{p^n} \leq (p-1) \sum_{n=1}^{\infty} \frac{1}{p^n} = 1 \quad \blacksquare$$

Consequently, each x in $[0, 1]$ can be so represented:

• **Proposition:**

Let p be an integer, $p \geq 2$, and let $0 \leq x \leq 1$. Then there is a sequence of integers $\{a_n\}$ with $0 \leq a_n \leq p-1$ for all n such that $x = \sum_{n=1}^{\infty} \frac{a_n}{p^n}$.

Proof:

Certainly the case $x = 0$ causes no real strain, so let us suppose that $0 < x \leq 1$. We will then construct $\{a_n\}$ by induction.

Choose a_1 to be the largest integer satisfying $\frac{a_1}{p} < x$. Since $x > 0$, it follows that $a_1 \geq 0$; and since $x \leq 1$, we have $a_1 < p$. Because a_1 is an integer, this means that $a_1 \leq p-1$. Also, since a_1 is largest, we must have

$$\frac{a_1}{p} < x \leq \frac{a_1+1}{p}.$$

Next, choose a_2 to be the largest integer satisfying $\frac{a_1}{p} + \frac{a_2}{p^2} < x$.

Check that $0 \leq a_2 \leq p-1$ and that

$$\frac{a_1}{p} + \frac{a_2}{p^2} < x \leq \frac{a_1}{p} + \frac{a_2+1}{p^2}.$$

Thus, by induction we get a sequence of integers $\{a_n\}$ with $0 \leq a_n \leq p-1$ such that

$$\frac{a_1}{p} + \dots + \frac{a_n}{p^n} < x \leq \frac{a_1}{p} + \dots + \frac{a_n+1}{p^n}$$

Obviously, $x = \sum_{n=1}^{\infty} \frac{a_n}{p^n}$. (Why??) ■

Note: The series $\sum_{n=1}^{\infty} \frac{a_n}{p^n}$ is called a base p (or p -adic) decimal expansion for x . It is sometimes written in the shorter form

$$x = 0.a_1 a_2 a_3 \dots \text{(base } p\text{)}.$$

It does not have to be unique (even for ordinary base 10 decimals: $0.5 = 0.4999\dots$). One problem is that our construction is designed to produce nonterminating decimal expansions. In the particular case where $x = \frac{a_1}{p} + \dots + \frac{a_n+1}{p^n} = \frac{q}{p^n}$, for some integer $0 < q \leq p^n$, the construction will give us a repeating string of $p-1$'s in the decimal expansion for x since $\frac{1}{p^n} = \sum_{k=n+1}^{\infty} \frac{p-1}{p^k}$. That is, any such x has two distinct base p decimal expansions:

$$x = \frac{a_1}{p} + \dots + \frac{a_n+1}{p^n} = \frac{a_1}{p} + \dots + \frac{a_n}{p^n} + \sum_{k=n+1}^{\infty} \frac{p-1}{p^k}$$

Notice that if $y \in \mathbb{R}$, for any $n \in \mathbb{N}$ we have $y \in [n, n+1]$. In particular, there is some $x \in [0, 1]$ such that $y = n + x$. By the work done above, this means that any real number y is an infinite sum of rational numbers.

Note: This is the end of our introductory discussion of the real line. The theorem below belongs to the complex realm and, since our focus on this course is on real numbers, this is the only theorem of complex variables that I will include in these notes (and I'm including it because of its relevance).

• **Theorem (Cauchy-Schwarz inequality):**

If a_1, \dots, a_n and b_1, \dots, b_n are complex numbers, then

$$\left| \sum_{j=1}^n a_j \bar{b}_j \right|^2 \leq \sum_{j=1}^n |a_j|^2 \sum_{j=1}^n |b_j|^2$$

Proof:

Let $A = \sum |a_j|^2$, $B = \sum |b_j|^2$, and $C = \sum a_j \bar{b}_j$.

If $B = 0$, then $b_1 = \dots = b_n = 0$, and the conclusion is trivial.

Therefore, assume $B > 0$. Then,

$$\begin{aligned} 0 \leq \sum |B a_j - C b_j|^2 &= \sum (B a_j - C b_j)(B \bar{a}_j - \bar{C} \bar{b}_j) \\ &= B^2 \sum |a_j|^2 - B \bar{C} \sum a_j \bar{b}_j - B C \sum \bar{a}_j b_j + |C|^2 \sum |b_j|^2 \\ &= B^2 A - B |C|^2 = B(A B - |C|^2) \end{aligned}$$

This implies that $A B - |C|^2 \geq 0$, so $A B \geq |C|^2$. ■