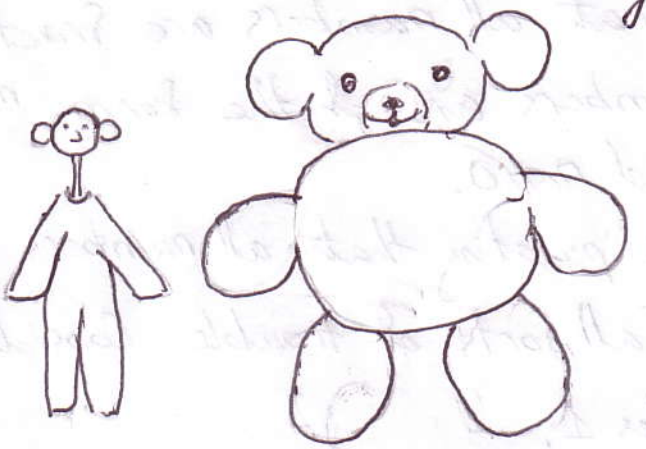
Chapter 1

The Real Number system

How important are numbers? To the pythagoreans, numbers were literally everything. And with good reason. The pythagoreans brought forth the hypothesis that all objects and their properties could, in principle, be deduced from one object alone. Here is how it might work.



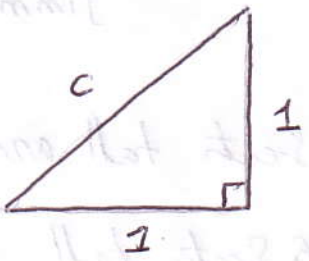
Tom Jimmy

Take Tom, he is $\frac{7}{2}$ feets tall and he loves his Teddy bear Jimmy who is 5 feets tall. But Tom is too young to know a foot as a unit of measurements (or perhaps he is European). He measures the world by Jimmy. Having a Chinese mathematics tutor, Tom can deduce that he is $\frac{7}{20}$ Jimmies tall and although Tom

has never seen a Giraffe, he can imagine her size when he is told that she is as tall as 3 Jimmies placed one upon the other.

Can Tom exclaim in the manner of Protagoras that Jimmy is the measure of all things? The answer may well depend on Tom's definition of number. By associating Jimmy with the number 1, Tom believes that the length of any other object could be communicated in terms of Jimmy. According to the pythagorean school of thought, this belief is equivalent to the assertion that all numbers are fractions of 1. That is, all numbers are of the form m/n, where m and n are integers and $n \neq 0$.

Unfortunately, stipulating that all numbers are rational fractions leads to all sorts of trouble. Consider the right triangle with sides 1,



The hypothenuse, whose length is c must satisfy the pythagorean equation $1^2+1^2=c^2$ or $c^2=2$. If all numbers are rational, then this equation has no solution as the following proposition implies.

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

Proof: Suppose that such a number does in fact exist. That is, suppose that there is a rational fraction $\frac{m}{n}$ such that

$$\left(\frac{m}{n}\right)^2 = p \qquad (1)$$

We can assume that this fraction is in simplest terms. In other words, that $\gcd(m, n) = 1$ (where gcd stands for greatest common divisor.)

Then equation (1) can be written as

$$m^2 = n^2 p \qquad (2)$$

which means that $p \mid m^2$ (p divides m^2). Thus $p \mid m$.

In particular, there exists an integer k such that $m = kp$, from which it follows that $m^2 = k^2 p^2 = n^2 p$ or

$$k^2 p = n^2 \qquad (3)$$

But this means that $p \mid n^2$ and therefore that $p \mid n$.

This is a contradiction, because $1 = \gcd(m, n) \geq p > 1$.

Thus, no rational fraction satisfying the equation $x^2 = p$ exists.

The conclusion of the above proposition is alarming. It seems to suggest the non-universality of the concept of length; If all numbers are rational and if a right triangle with sides of length 1 exists, then either the hypothenuse has no length or its length is of a radically different sort and therefore incommensurable with the length of the sides of the right triangle.

We can try to escape this conundrum by denying that roots of prime numbers exist, but this does not seem to agree with the physics of nature.

Ex. Suppose that you are standing somewhere on the street when a clumsy construction worker drops a brick 5ft above your head.

The position of the brick is given by $p(t) = 16t^2$. It will land on your head precisely when $p(t) = 5$. But this would imply that the time of impact must satisfy the equation $(4t)^2 = 5$ or when $4t = \sqrt{5}$. If you do not believe in roots of prime numbers, then you have no reason to fear the falling brick. No time t satisfies the equation and therefore the brick will never hit you. Would you be willing to do an experiment?

Ex. It turns out that even cops believe in roots of prime numbers. As I was flipping through the channels, I stumbled upon a show called "Ice Road Truckers" and was captivated by what I saw.

A truck-driver was bitterly arguing with a police officer about a speeding ticket. The officer was giving him a ticket even though the driver was never caught in the act. The officer had no eyewitnesses and no data from radar or traffic cameras. In fact there was no direct, first hand evidence that the truck moved at all. What gives this cop the right to write a speeding ticket?

Suppose that the trucker must drive from station A to station B that is 60 miles further down the road. He clocks in at the start of the drive, say 12:00 ($t=0$)

and clocks out upon arrival at station B one hour later ($t=1$). Suppose that the speed limit is 55 mi/hr.

Station A
$(t=0)$
$p(0)=0$

$p(t)=?$

Station B
$(t=1)$
$p(1)=60$

Although the driver was never observed on the road and therefore his position function $p(t)$ is not known, the officer can compute the trucker's average velocity to be

$$\frac{p(1)-p(0)}{1-0} = 60 \text{ mi/hr.}$$

This, however, is just the average velocity. It tells us that the trucker must have been speeding if the velocity throughout his journey was constant. But there is no data about the driver's actual motion and it seems highly unlikely that the truck's speed never changed.

At this point, the police officer may recall the mean value theorem, taught to him in the police academy. If p is continuous on $[0,1]$ and differentiable on $(0,1)$ then

$$60 = \frac{p(1)-p(0)}{1-0} = p'(t)$$

for some $t \in (0,1)$. In other words, the mean value theorem implies that at some moment in the journey, the actual velocity of the truck must have been equal to the average velocity.

The mean value theorem is a fairly solid mathematical argument. Does it justify the traffic violation ticket then? Let $p(t) = 60t^3$. Then $p(0) = 0$ and $p(1) = 60$ so p could have been the position function of the truck driver on the road. Now

$$60 = \frac{p(1)-p(0)}{1-0} = p'(t) = 180t^2.$$

Thus, the time when the truck driver matches the average velocity is $t = \frac{1}{\sqrt{3}}$. If you think that $\sqrt{3}$ does not exist, try convincing a policeman. They are difficult to argue with.

Ex. Functions constructed on rational fractions are often not sufficiently descriptive even when it comes to predicting terms in a sequence of integers. To determine an integer as a function of another integer, one may need to resort to roots of prime numbers:

Consider the Fibonacci number sequence.

$F(1) = 1$, $F(2) = 1$ and $F(n+2) = F(n) + F(n+1)$

where $F(n)$ is the n^{th} Fibonacci number identified by some function $F: \mathbb{N} \to \mathbb{N}$.

It can be shown that

$$F(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n \sqrt{5}}$$

which is meaningless if $\sqrt{5}$ is not a number.

These examples show that the rational number system is inadequate for many purposes and must therefore be expanded. Let's denote the set of rational numbers with the letter $\mathbb{Q}$. As it turns out, the observation below reveals the property which $\mathbb{Q}$ is lacking. By constructing a set $\mathbb{R}$ from $\mathbb{Q}$ and equipping it with the missing property we will patch

the number system (for the time being)

Observation: Let p be a prime number. Set $A = \{r \in \mathbb{Q}^+ : r^2 < p\}$ and $B = \{r \in \mathbb{Q}^+ : r^2 > p\}$, where $\mathbb{Q}^+$ is the set of all positive rational numbers. Then, for each $r \in A$, there exists $s \in A$ such that $r < s$. Similarly, for each $r \in B$, there is some $s \in B$ such that $s < r$. More explicitly, define

$$s = r - \frac{r^2 - p}{r + p} \qquad (1)$$

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 $r > s$. Notice that

$$s^2 - p = \frac{(r^2 p - p^2)(p-1)}{(r+p)^2} \qquad (2)$$

Thus, if $r \in A$, then $r^2 p - p^2 < p^2 - p^2 = 0$. In particular, if $r \in A$, then $s \in A$. If $r \in B$, then $r^2 p - p^2 > p^2 - p^2 = 0$, implying that $s \in B$.

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 $\mathbb{Q}$): for any $s \in B$, there is $s_1 < s$ 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.

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

(i) If $x \in S$ and $y \in S$ then one and only one of the statements

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

is true.

(ii) If $x, y, z \in S$, if $x < y$ and $y < z$, then $x < z$.

It is often convenient to write $y > x$ in place of $x < y$. The notation $x \leq y$ indicates that $x < y$ or $x = y$, without specifying which of these two is to hold. In other words, $x \leq y$ is the negation of $x > y$.

Def: An ordered set is a set S in which an order 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.

Def: Suppose S is an ordered set, and $E \subset S$. If there exists a $\beta \in S$ such that $x \leq \beta$ for every $x \in E$, 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 $\leq$).

Def: Suppose S is an ordered set, $E \subset S$, and E is bounded above. 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 of E (that there is at most one such α is clear from (ii)) or the supremum of E, and we write

$$\alpha = \sup E.$$

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.

Ex. (a) Consider the sets A and B described earlier 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

$$\sup E_1 = \sup E_2 = 0.$$

and $0 \notin E_1$, $0 \in E_2$.

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

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

Def: 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. 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.

Thm: Suppose S is an ordered set with the least-upper-bound property, $B \subset S$, B is not empty, and B is bounded below. 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 not empty. Since L consists of exactly those $y \in S$ which satisfy the inequality $y \leq x$ for all $x \in B$, we see that every $x \in B$ is an upper bound of L. Thus 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 $\alpha \leq x$ for every $x \in B$. It follows that $\alpha \in L$.

If $\alpha < \lambda$ then $\lambda \notin L$, since α is an upper bound of L.

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 means that $\alpha = \inf B$.

Before going on, you should review the definitions of ordered field and field axioms.

We may now state the existence theorem which allows us to extend the rational number system.

Thm: There exists an ordered field $\mathbb{R}$ which has the least-upper-bound property.

Moreover, $\mathbb{R}$ contains $\mathbb{Q}$ as a subfield.

Proof: The proof is found in the appendix of Chapter 1 of "Principles of mathematical Analysis".

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

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

$$nx > y$$

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

Part (a) is usually referred to as the archimedian 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: Set $A = \{nx : n \in \mathbb{N}\}$. If (a) were false, then y would be an upper bound of A. Put $\alpha = \sup A$. Since $x > 0$, $\alpha - x < \alpha$ and $\alpha - x$ is not an upper bound of A. Hence $\alpha - x < mx$ for some positive integer m. But then $\alpha < (m+1)x \in A$, which contradicts the statement that $\alpha = \sup A$. 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

$$m - 1 \leq nx < m$$

Observe also that

$$m \leq 1 + nx < ny$$

Thus, since $nx < m$, we have

$$nx < m < ny$$

In particular

$$x < \frac{m}{n} < y.$$

This proves (b), with $p = \frac{m}{n}$.

We are now ready to prove the existance of n^{th} roots of positive reals.

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

Proof 1 (Rudin): That there is at most one such y is clear, since $0 < y_1 < y_2$ implies $y_1^n < y_2^n$.

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

If $t = \frac{x}{1+x}$ then $0 \leq t < 1$. Hence $t^n \leq t < x$. Thus $t \in E$, and 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 there exists $y = \sup E$.

To prove that $y^n = x$ we will show that each of the inequalities $y^n < x$ and $y^n > x$ leads to a contradiction.

The identity $b^n - a^n = (b-a)(b^{n-1} + b^{n-2}a + \ldots + a^{n-1})$ yields the inequality.

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

when $0 < a < b$.

Assume $y^n < x$. Choose h so that $0 < h < 1$ and

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

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

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

In particular,

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

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

Assume $y^n > x$. Put

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

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

In particular, $0 < k < y$.

Thus,

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

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 $y^n = x$, and the proof is complete.

Proof 2 (mine): Let E be as before. Follow the arguments of proof 1 to show that E is not empty and bounded above. 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 $y^n = x$.

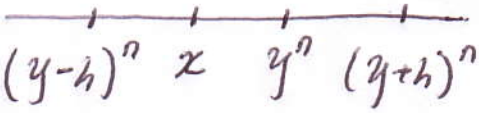
Let $h > 0$. If $h < y$ then $y-h$ is a positive number that is not an upper bound of E. In particular, there is some $t \in E$ such that $y-h < t < y$ and therefore

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

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

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

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

where $\lfloor \alpha \rfloor$ is the floor function (i.e. a function that rounds α down to the nearest integer). 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: Put $\alpha = a^{1/n}$, $\beta = b^{1/n}$. Then

$$ab = \alpha^n \beta^n = (\alpha\beta)^n$$

since multiplication is commutative. The uniqueness assertion of the previous theorem shows that

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

So what are real numbers? The following propositions give some insights.

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:

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

Conversely, 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 construct $\{a_n\}$ by induction. By the archemedian property, we can choose an integer a_1 such that $\frac{a_1}{p} < x$ and $\frac{a_1+1}{p} \geq x$. 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 $a_1 \leq p-1$.
Next, choose a_2 to be the largest integer satisfying $\frac{a_1}{p} + \frac{a_2}{p^2} < x$. Specifically, use the archemedian property to find an integer a_2+1 such that $\frac{a_2}{p^2} < x - \frac{a_1}{p} \leq \frac{a_2+1}{p^2}$. Since $x - \frac{a_1}{p} > 0$, it follows that $a_2 \geq 0$; since $\frac{a_1+1}{p} \geq x$, we have $a_2 \leq p-1$ (why?)
We see that

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

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

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

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

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 $x = 0.a_1a_2a_3\ldots$ (base p). It does not have to be unique (even for ordinary base 10 decimals: $0,5 = 0,4999\ldots$)

Notice that if $y \in \mathbb{R}$, then $y \in [n, n+1]$. 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.

This is good news! By modifying the pythagorean definition of number, it appears that we may once again assert that all is number. In particular, Tom may rekindle his belief that Jimmy is the measure of all things at a small cost; Tom must allow the description of the world in terms of Jimmy to be infinite.

The Complex number system.

We have seen that rational numbers have certain gaps. We have filled these gaps by extending the rational number system $\mathbb{Q}$ to the real number system $\mathbb{R}$. Must $\mathbb{R}$ be further extended? The real number system allows us to take roots of any positive numbers. How about taking roots of negative numbers? On first glance, this question seems ludicrous. You have learned that if $x \geq 0$, then $x^2 \geq 0$ and if $x < 0$, then $x^2 > 0$. If there is some x such that $x^2 = -1$, wouldn't it imply that $0 \leq x^2 = -1$?

Many great mathematicians were happy to maintain that equations like $x^2 + 1 = 0$ are simply meaningless. There is a problem with this view.

Have you heard the famous expression "A philosopher is a blind man in a dark room, searching for a black cat that is not there"? You might think that this philosopher is wasting his time, but you are wrong! Suppose that the number of black cats in the room is a solution to the equation

$$x^3 - 15x - 4 = 0$$

This equation is of the form

$$x^3 + px + q = 0$$

where $p = -15$ and $q = -4$.

Applying Cardano's cubic formula to $x^3+px+q=0$ yields

$$x = \sqrt[3]{\frac{1}{2}\left(-q+\sqrt{q^2+\frac{4p^3}{27}}\right)} + \sqrt[3]{\frac{1}{2}\left(-q-\sqrt{q^2+\frac{4p^3}{27}}\right)}$$

Since $p=-15$ and $q=-4$, the above equation reduces to

$$x = \sqrt[3]{2+\sqrt{-121}} + \sqrt[3]{2-\sqrt{-121}}$$

If there are no roots of negative numbers, then root of -121 does not exist and the proposed solution is a laughable waste of time. Suppose, however, that root of -1 does exist. Call it $i=\sqrt{-1}$ (because we imagine that it does). Then $\sqrt{-121} = \sqrt{-1}\sqrt{121} = 11i$. Therefore

$$x = \sqrt[3]{2+11i} + \sqrt[3]{2-11i}.$$

Since we are assuming that $i^2=-1$, it can be shown that $(2+i)^3 = 2+11i$ and $(2-i)^3 = 2-11i$ (if you are interested to hear the details, ask me after class). Thus

$$x = \sqrt[3]{(2+i)^3} + \sqrt[3]{(2-i)^3} = 2+i+2-i = 4.$$

Does this make sense? Observe that $4^3-15\cdot 4-4=0$. Hence 4 is a solution to $x^3-15x-4=0$,

By imagining that a black cat is in the room, the philosopher actually finds four of them.

We now develop the theory of the complex number Field.

Def: A complex number is an ordered pair (a,b) of real numbers. "Ordered" means that (a,b) and (b,a) are regarded as distinct if $a \neq b$.

Let $x=(a,b)$, $y=(c,d)$ be two complex numbers. We write $x=y$ iff $a=c$ and $b=d$.

define $$x+y = (a+c,\ b+d)$$

$$xy = (ac-bd,\ ad+bc)$$

You should verify that these definitions of addition and multiplication turn the set of complex numbers into a field, with $(0,0)$ and $(1,0)$ in the role of 0 and 1.

Thm: For any real numbers a and b we have

$$(a,0)+(b,0) = (a+b,0)\ ,\quad (a,0)(b,0) = (ab,0).$$

Thus the real numbers may be viewed as a subset of complex numbers, if we agree to identify $(a,0)$ with a.

Def: $i = (0,1)$

Thm: $i^2 = -1$

Proof: $i^2 = (0,1)(0,1) = (-1,0) = -1$

We now show that the traditional representation of complex numbers as $a+bi$ is equivalent to (a,b).

Thm: If a and b are real, then $(a,b) = a+bi$

Proof: $a+bi = (a,0)+(b,0)(0,1) = (a,0)+(0,b) = (a,b)$.

Def: If a, b are real and $z = a+bi$, then the complex number $\bar{z} = a-bi$ is called the conjugate of z. The numbers a and b are the real part and the imaginary part of z, respectively. We shall write

$$a = Re(z), \quad b = Im(z)$$

Thm: If z and w are complex, then

(a) $\overline{z+w} = \bar{z} + \bar{w}$

(b) $\overline{zw} = \bar{z} \cdot \bar{w}$

(c) $z+\bar{z} = 2\,Re(z)$, $z-\bar{z} = 2i\,Im(z)$

(d) $z\bar{z} = a^2+b^2$ if $z = a+bi$

Def: If z is a complex number, its absolute value $|z|$ is the non-negative square root of $z\bar{z}$; that is, $|z| = (z\bar{z})^{1/2}$. The existence (and uniqueness) of $|z|$ follows from the real root theorem.

Note that when x is real, then $\bar{x} = x$, hence $|x| = \sqrt{x^2}$.

Thus $|x| = x$ if $x \geq 0$, $|x| = -x$ if $x < 0$.

Thm: Let z and w be complex numbers. Then

(a) $|z| > 0$ unless $z = 0$, $|0| = 0$

(b) $|\bar{z}| = |z|$

(c) $|zw| = |z||w|$

(d) $|\mathrm{Re}\, z| \leq |z|$

(e) $|z+w| \leq |z| + |w|$

Proof: (a) and (b) are trivial. Put $z = a+bi$, $w = c+di$, with a, b, c, d real. Then

$$|zw|^2 = (ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2) = |z|^2|w|^2$$

or $|zw|^2 = (|z||w|)^2$. (c) follows from the assertion that real roots are unique.

To prove (d), note that $a^2 \leq a^2+b^2$, hence

$$|a| = \sqrt{a^2} \leq \sqrt{a^2+b^2}.$$

To prove (e), note that $\bar{z}w$ is the conjugate of $z\bar{w}$, so that $z\bar{w} + \bar{z}w = 2\,\mathrm{Re}(z\bar{w})$. Hence

$$|z+w|^2 = (z+w)(\bar{z}+\bar{w}) = z\bar{z} + z\bar{w} + \bar{z}w + w\bar{w} =$$

$$= |z|^2 + 2\,\mathrm{Re}(z\bar{w}) + |w|^2 \leq |z|^2 + 2|z\bar{w}| + |w|^2 =$$

$$= |z|^2 + 2|z||w| + |w|^2 = (|z| + |w|)^2.$$

(e) follows by taking square roots.

Notation: If $x_1, \ldots, x_n$ are complex numbers, we write

$$x_1 + x_2 + \ldots + x_n = \sum_{j=1}^{n} x_j$$

The following important theorem is known as the Cauchy-Schwarz inequality.

Thm: If $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ 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: Put $A = \sum |a_j|^2$, $B = \sum |b_j|^2$, $C = \sum a_j \bar{b}_j$.

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

Assume $B > 0$. Then

$$0 \leq \sum |Ba_j - Cb_j|^2 = \sum (Ba_j - Cb_j)(B\bar{a}_j - C\bar{b}_j) =$$

$$= B^2 \sum |a_j|^2 - B\bar{C} \sum a_j \bar{b}_j - BC \sum \bar{a}_j b_j + |C|^2 \sum |b_j|^2$$

$$= B^2 A - B|C|^2 = B(AB - |C|^2)$$

This implies that $AB - |C|^2 \geq 0$ so $AB \geq |C|^2$.